Configuring IPX Services

Router Software Version 10.0
Site Manager Software Version 4.0

Part No. 112918 Rev. A
January 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. January 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, BCN, BLN, BN, CN, FRE, LN, Optivity, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and AN, ANH, ASN, BaySIS, BayStack, BCNX, BLNX, BNX, EZ Internetwork, EZ LAN, FN, PathMan, PhonePlus, PPX, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: *This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.*

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Audience xv
Before You Begin xvi
Bay Networks Customer Support xvi
CompuServe xvi
InfoFACTS xvii
World Wide Web xvii
How to Get Help xviii
Conventions xviii
Ordering Bay Networks Publications xix
Acronyms xix

Chapter 1
IPX Overview

Compatibility with Previous Versions of Bay Networks Software 1-1
About the IPX Protocol 1-2
Supported LAN Circuits, WAN Circuits, and Frame Formats 1-3
Network-Level Services 1-4
Multiple IPX Interfaces per Circuit 1-5
IPX over WAN Media 1-6
Using IPXCP and IPXWAN 1-7
Running IPXWAN over PPP 1-7
Running IPXWAN over Frame Relay Permanent Virtual Circuits 1-8
Negotiating an IPXWAN Connection 1-8
IPX Network Numbers 1-8
Primary Network Number 1-9
Common Network Number 1-9
Router Names 1-10
Sample IPXCP and IPXWAN Configurations 1-10

IPXCP Link Negotiation 1-11
IPXWAN Link Negotiation 1-12
IPXWAN and IPXCP Link Configurations 1-12
Configuration 1 (IPXWAN with IPXCP on Both Interfaces) 1-13
Configuration Guidelines — Configuration 1 1-13
Configuration 2 (IPXWAN on Both Interfaces) 1-13
Configuration Guidelines — Configuration 2 1-13
Configuration 3 (Only IPXCP on Both Interfaces) 1-14
Configuration Guidelines — Configuration 3 1-14
Configuration 4 1-14
Handling Packets Associated with Upper-Layer Protocols 1-14
Routing Information Protocol (RIP) 1-15
IPX Route Filters 1-17
Configuring RIP and SAP Broadcast Timers 1-17
Routing Methods 1-19
Configuring Interface Costs 1-19
Configurable RIP Timers 1-20
Multipath Routing and Load sharing 1-22
Multipath Routing 1-22
Load Redistribution and Rerouting 1-24
Multipath Route Precedence/Priority 1-25
Multipath Configurations 1-25
Multiline Circuits 1-25
Configurable Split Horizon 1-26
Fully Meshed Networks 1-27
Nonfully Meshed Networks 1-27
Static Route Support 1-28
Default Route Support 1-30
Adjacent Host Support 1-31
Service Advertising Protocol (SAP) 1-32
NetWare Directory Services (NDS) and SAP 1-33
SAP and the NetWare Bindery (NetWare 3.*x* and Earlier) 1-33
Configurable SAP Timers 1-34
Configuring SAP Filters 1-35
Static Services 1-37

Dial-on-Demand 1-40
Using Dial-on-Demand Service 1-41
Using Static Routing with Dial-on-Demand 1-43
Tips for Using Dial-on-Demand with IPX 1-43
Local IPX Watchdog Acknowledgment 1-43
NetBIOS Static Routing 1-44
Directing a NetBIOS Packet Using Nonstandard Static Routing 1-46
Forwarding Packets Out All Interfaces 1-47
Directing a NetBIOS Packet Using Standard Static Routing 1-48
NetBIOS Broadcast Filters 1-49
Source Route Bridge Endstation Support 1-52
IPX Ping Support 1-54
Role of Bay Networks Routers in a Client/Server Connection 1-55
Example of Client/Server Connection via Bay Networks Router 1-56
For More Information about IPX 1-58

Chapter 2
IPX Configuration and Parameter Requirements

Standard IPX Configurations 2-1
Multiple-Host Router 2-1
Single-Host Router 2-2
Special IPX Configurations 2-2
Multiple Interfaces per Circuit 2-2
Multiple-Host Addressing, Host Numbers, and MAC Addresses 2-3
Network Numbers 2-3
Frame Encapsulation Types and the Number of IPX Interfaces per Circuit 2-4
Multiple Circuits per Segment 2-5
IPX Host ID Numbers 2-5
Host ID Number for IPX on a Token Ring Circuit 2-6
Token Ring MAC Address Selection 2-7
Host ID Number for IPX over ATM 2-8
Configuring IPX without RIP 2-8

Chapter 3

Enabling IPX and IPXWAN Services

Enabling IPX and IPXWAN on a Circuit 3-1

IPX and IPXWAN Parameter Descriptions 3-3
Accepting or Editing the Default Configuration Parameter Values 3-7

Chapter 4
Editing IPX Parameters

Accessing IPX Parameters Using the Technician Interface 4-2
Accessing IPX Parameters Using Site Manager 4-2
Editing IPX Global Parameters 4-3
IPX Global Parameter Descriptions 4-5
Editing IPX Advanced Global Parameters 4-9
IPX Advanced Global Parameter Descriptions 4-10
Editing IPX Interface Parameters 4-17
IPX Interface Parameter Descriptions 4-19
Editing IPX Change Circuit Parameters 4-26
IPX Change Circuit Parameter Descriptions 4-27
Editing IPX RIP Circuit Parameters 4-30
IPX RIP Circuit Parameter Descriptions 4-32
Editing IPX SAP Circuit Parameters 4-37
IPX SAP Circuit Parameter Descriptions 4-38
Using NetBIOS Static Routes 4-42
Adding a NetBIOS Static Route 4-43
IPX NetBIOS Static Route Configuration Parameter Descriptions 4-44
Editing a NetBIOS Static Route 4-46
IPX NetBIOS Static Route Parameter Descriptions 4-46
Deleting a NetBIOS Static Route 4-47
Editing Adjacent Host Parameters 4-47
Adding an Adjacent Host 4-49
Adjacent Host Configuration Parameter Descriptions 4-50
Editing an Adjacent Host 4-51
IPX Adjacent Hosts Parameter Descriptions 4-51
Deleting an Adjacent Host 4-52
Using Static Routes 4-52
Adding a Static Route 4-54
Adding a Default Route 4-54
IPX Static Route Configuration Parameter Descriptions 4-55
Editing a Static Route 4-56

IPX Static Route Parameter Descriptions 4-56
Deleting a Static Route 4-58
Using Static Services 4-58
Adding a Static Service 4-59
IPX Static Service Configuration Parameter Descriptions 4-60
Editing a Static Service 4-63
IPX Static Service Parameter Descriptions 4-63
Deleting a Static Service 4-65
Using Route Filters 4-66
Adding a Route Filter 4-69
Editing Route Filter Configuration Parameters 4-69
Editing an IPX Route Filter 4-71
IPX Route Filter Parameter Descriptions 4-71
Deleting an IPX Route Filter 4-75
Using SAP Filters 4-76
Using Wildcards and Pattern Matching with SAP Filters 4-76
Using Wildcards with SAP Filters 4-77
Using Pattern Matching with SAP Filters 4-77
An Example of Using SAP Filters 4-81
Configuring Service Network Filters 4-81
Adding a Service Network Filter 4-84
Service Network Filter Configuration Parameter Descriptions 4-84
Editing a Service Network Filter 4-86
IPX Service Network Filter Parameter Descriptions 4-87
Deleting a Service Network Filter 4-91
Editing Service Name Filter Parameters 4-92
Adding a Service Name Filter 4-93
IPX Service Name Filter Configuration Parameter Descriptions 4-94
Editing a Service Name Filter 4-96
IPX Service Name Filter Parameter Descriptions 4-97
Deleting a Service Name Filter 4-101
Deleting IPX from the Router 4-102

Appendix A
Common Service Types and Identifiers

Appendix B
IPX Default Parameter Settings

IPX Global Parameter Defaults B-1
IPX Advanced Global Parameter Default Values B-2
IPX Interface Parameter Default Values B-2
IPX Change Circuit Parameter Default Values B-3
IPX RIP Circuit Parameter Default Values B-4
IPX SAP Circuit Parameter Default Values B-4
IPX NetBIOS Static Route Configuration Parameter Default Values B-5
IPX NetBIOS Static Route Parameter Default Values B-5
Adjacent Host Configuration Parameter Default Values B-6
IPX Adjacent Hosts Parameter Default Values B-6
IPX Static Route Configuration Parameter Default Values B-6
IPX Static Route Parameter Default Values B-7
IPX Static Service Configuration Parameter Default Values B-7
IPX Static Services Parameter Default Values B-8
Route Filter Configuration Parameter Default Values B-8
IPX Route Filter Parameter Default Values B-9
SAP Network Filter Configuration Parameters B-10
IPX SAP Network-Level Filter Parameter Descriptions B-10
IPX Server-Level Filter Configuration Parameter Descriptions B-11
IPX SAP Server-Level Parameter Default Values B-11

Appendix C
Sample IPX Configuration

Configuration Particulars C-3
Router 1 ..... C-3
Router 2 ..... C-3

Index

Figures

Figure 1-1. Multiple IPX Interfaces per Physical Circuit 1-6
Figure 1-2. IPXCP and IPXWAN Configurations 1-11
Figure 1-3. IPX Configurable RIP Interface Cost 1-20
Figure 1-4. IPX Configurable RIP Timers 1-21
Figure 1-5. IPX Multipath 1-23
Figure 1-6. IPX Multipath Routing — Equal Least-Cost Routes 1-24
Figure 1-7. Split Horizon Enabled in a Fully Meshed Network 1-27
Figure 1-8. Split Horizon Disabled in a Nonfully Meshed Network 1-28
Figure 1-9. IPX Static Routes 1-30
Figure 1-10. Using IPX Adjacent Hosts to Reduce Manual Configuration 1-32
Figure 1-11. SAP Filtering 1-36
Figure 1-12. Static SAP Service Network Configuration 1-39
Figure 1-13. IPX SAP Filters Prohibiting SAP Broadcasts 1-40
Figure 1-14. Dial-on-Demand Service 1-42
Figure 1-15. NetBIOS Static Routes 1-46
Figure 1-16. IPX Interfaces Window 1-48
Figure 1-17. NetBIOS Packet Filtering 1-50
Figure 1-18. NetBIOS Packet Flow 1-51
Figure 1-19. NetBIOS Broadcast Filtering 1-52
Figure 1-20. IPX Routers Source Routing across a Token Ring Network 1-53
Figure 1-21. Sample IPX Network 1-57
Figure 2-1. Frames Received at a Logical Interface 2-5
Figure 2-2. Frames Issued from a Logical Interface 2-6
Figure 3-1. IPX Configuration Window 3-2
Figure 3-2. IPX Configuration Window for a Specific Interface 3-7
Figure 4-1. Configuration Manager Window 4-3
Figure 4-2. Edit IPX Global Parameters Window 4-4
Figure 4-3. Edit IPX Advanced Global Parameters Window (Top) 4-9

Figure 4-4. Edit IPX Advanced Global Parameters Window (Bottom) 4-10
Figure 4-5. IPX Interfaces Window 4-18
Figure 4-6. IPX Change Circuit Window 4-26
Figure 4-7. IPX RIP Circuit Window (Top) 4-31
Figure 4-8. IPX RIP Circuit Window (Bottom) 4-32
Figure 4-9. IPX SAP Circuit Window (Top) 4-37
Figure 4-10. IPX NetBIOS Static Routes Window 4-43
Figure 4-11. IPX NetBIOS Static Route Configuration Window 4-44
Figure 4-12. IPX Static Interface Tables Configuration Window 4-48
Figure 4-13. IPX Adjacent Hosts Window 4-48
Figure 4-14. IPX Adjacent Host Configuration Window 4-49
Figure 4-15. IPX Static Routes Window 4-53
Figure 4-16. IPX Static Route Configuration Window 4-54
Figure 4-17. IPX Static Services Window 4-59
Figure 4-18. IPX Static Service Configuration Window 4-60
Figure 4-19. IPX Route Filters Window (Top) 4-67
Figure 4-20. IPX Route Filters Window (Bottom) 4-68
Figure 4-21. IPX Route Filter Configuration Window 4-69
Figure 4-22. IPX Service Network Filters Window (Top) 4-82
Figure 4-23. IPX Service Network Filters Window (Bottom) 4-83
Figure 4-24. IPX Service Network Filter Configuration Window 4-84
Figure 4-25. IPX Service Name Filters Window (Top) 4-92
Figure 4-26. IPX Service Name Filters Window (Bottom) 4-93
Figure 4-27. IPX Service Name Filter Configuration Window 4-94
Figure C-1. Sample IPX Configuration C-2

Tables

Table 1-1. LAN Circuit and Frame Support for IPX Interfaces 1-3
Table 1-2. WAN Circuit and Frame Support for IPX Interfaces 1-3
Table 1-3. Configuration Table for IPX Over WAN Media 1-12
Table 4-1. Characters in SAP Pattern Matching Filters 4-78
Table 4-2. Concatenation Rules and Operators 4-79
Table A-1. Service Types and Identifiers A-1
Table B-1. IPX Global Parameter Default Values B-1
Table B-2. IPX Advanced Global Parameter Default Values B-2
Table B-3. IPX Interface Parameter Default Values B-2
Table B-4. IPX Change Circuit Parameter Default Values B-3
Table B-5. IPX RIP Circuit Parameter Default Values B-4
Table B-6. IPX SAP Circuit Parameter Default Values B-4
Table B-7. NetBIOS Static Route Configuration Parameter Default Values B-5
Table B-8. IPX NetBIOS Static Route Parameter Default Values B-5
Table B-9. Adjacent Host Configuration Parameter Default Values B-6
Table B-10. IPX Adjacent Hosts Parameter Default Values B-6
Table B-11. IPX Static Route Configuration Parameter Default Values B-6
Table B-12. IPX Static Route Parameter Default Values B-7
Table B-13. IPX Static Service Configuration Parameter Default Values B-7
Table B-14. IPX Static Services Parameter Default Values B-8
Table B-15. Route Filter Configuration Parameter Default Values B-8
Table B-16. IPX Route Filter Parameter Default Values B-9
Table B-17. SAP Network Filter Configuration Parameter Default Values B-10
Table B-18. SAP Network-Level Filter Parameter Default Values B-10
Table B-19. IPX Server-Level Filter Configuration Parameter Default Values B-11
Table B-20. IPX SAP Server-Level Parameter Default Values B-11

About This Guide

If you are responsible for configuring and managing Bay Networks™ routers, read this guide to discover how to customize Bay Networks router software for Internet Packet Exchange (IPX) services.

Customizing IPX Services offers

- An overview of the IPX protocol and a description of how Bay Networks routing services work (refer to Chapter 1)
- Implementation notes that may affect how you configure IPX routing services (refer to Chapter 2)
- Instructions on enabling IPX and IPXWAN (refer to Chapter 3)
- Instructions on editing IPX global and interface parameters and configuring IPX services (refer to Chapter 4)

For information and instructions about the following tasks, see *Configuring Routers*:

- Retrieving a configuration file
- Rebooting the router with a configuration file

Audience

Written for system and network managers, this guide describes how to configure the Bay Networks implementation of IPX interfaces to suit your environment.

Whether you use Novell computers or a combination of Novell and compatible third-party systems, this guide provides the options you need to communicate and share resources on your network.

Before You Begin

Before using this guide, you must complete the following procedures:

- Create and save a configuration file that has at least one IPX interface.
- Retrieve the configuration file in local, remote, or dynamic mode.

Refer to *Configuring Routers* for instructions.

Bay Networks Customer Support

Bay Networks provides live telephone technical support to our distributors, resellers, and service-contracted customers from two U.S. and three international support centers. If you have purchased your Bay Networks product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues.

Customers also have the option of purchasing direct support from Bay Networks through a variety of service programs. The programs include priority access telephone support, on-site engineering assistance, software subscription, hardware replacement, and other programs designed to protect your investment.

To purchase any of these support programs, including PhonePlus™ for 24-hour telephone technical support, call 1-800-2LANWAN. Outside the U.S. and Canada, call (408) 764-1000. You can also receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your reseller. Bay Networks provides several methods of receiving support and information on a nonpriority basis through the following automated systems.

CompuServe

Bay Networks maintains an active forum on CompuServe. All you need to join us online is a computer, a modem, and a CompuServe account. We also recommend using the CompuServe Information Manager software, available from CompuServe.

The Bay Networks forum contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. Software agents and patches are available, and the message boards are monitored by technical staff and can be a source for problem solving and shared experiences.

Customers and resellers holding Bay Networks service contracts can visit the special libraries to acquire advanced levels of support documentation and software.

To open an account and receive a local dial-up number, call CompuServe at 1-800-524-3388 and ask for Representative No. 591.

- In the United Kingdom, call Freephone 0800-289378.
- In Germany, call 0130-37-32.
- In Europe (except for the United Kingdom and Germany), call (44) 272-760681.
- Outside the U.S., Canada, and Europe, call (614) 529-1349 and ask for Representative No. 591, or consult your listings for an office near you.

Once you are online, you can reach our forum by typing the command GO BAYNETWORKS at any ! prompt.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system can return a fax copy to the caller or to a third party within minutes of being accessed.

World Wide Web

The World Wide Web (WWW) is a global information system for file distribution and online document viewing via the Internet. You need a direct connection to the Internet and a Web Browser (such as Mosaic or Netscape).

Bay Networks maintains a WWW Home Page that you can access at http://www.baynetworks.com. One of the menu items on the Home Page is the Customer Support Web Server, which offers technical documents, software agents, and an E-mail capability for communicating with our technical support engineers.

How to Get Help

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-005

Conventions

This section describes the conventions used in this guide.

arrow character (➔)	Separates menu and option names in instructions. Example: Protocols➔AppleTalk identifies the AppleTalk option in the Protocols menu.
bold text	Indicates text that you need to enter and command names in text. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers. You may also request a free catalog of Bay Networks Press product publications.

Phone:	1-800-845-9523
FAX - U.S./Canada:	1-800-582-8000
FAX - International:	1-916-939-1010

Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asychronous Transfer Mode
CMIP	Common Management Information Protocol
CNN	Common Network Number
CSU	Channel Service Unit
DLCI	data link connection identifier
EGP	Exterior Gateway Protocol
FDDI	Fiber Distributed Data Protocol
FTP	File Transfer Protocol
HDLC	high-level data link control
HSSI	high-speed serial interface
IDP	Internet Data Packet
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPX	Internet Packet Exchange
ISDN	Integrated Services Digital Network
LAN	local area network
LMI	Local Management Interface
LQR	Link Quality Reporting
LSAP	(Data) Link Layer Service Access Point
MAC	Media Access Control
MAU	media access unit

MIB	Management Information Base
MOP	Maintenance Operations Protocol
MTU	Maximum Transmission Unit
NBMA	Non-Broadcast Multi-Access
NCP	Network Control Protocol
NDS	NetWare Directory Services
NIC	network interface card
NMM	network management module
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PNN	Primary Network Number
PPP	Point-to-Point Protocol
PROM	Programmable Read-Only Memory
PVC	permanent virtual circuit
QWNET	Quad Ethernet Link Module
RARP	Reverse Address Resolution Protocol
RFC	Request for Comments
RIF	Routing Information Field
RIP	Routing Information Protocol
RMON	remote monitoring
SAM	System Administration Manager
SAP	Service Advertising Protocol
SMDS	Switched Multimegabit Data Services
SMIT	System Management Interface Tool
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SRE	Single Route Explorer
SVC	switched virtual circuit
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunication Network
TFTP	Trivial File Transfer Protocol
TFTPD	Trivial File Transfer Protocol Daemon
UDP	User Datagram Protocol

UTP	unshielded twisted pair
WAN	wide area network
XNS	Xerox Network System

Chapter 1
IPX Overview

This chapter gives you an overview of how the Internet Packet Exchange (IPX) protocol works with Bay Networks routers. The first part of the chapter deals with the IPX protocol itself, its requirements, and its place in the OSI model. The latter part of the chapter describes how IPX packets flow across an internetwork. Subsequent chapters give details on implementing and enabling IPX on your routers, and on specifying and editing IPX parameters.

Compatibility with Previous Versions of Bay Networks Software

This guide describes only the Version 10.0 Bay Networks router software.

Site Manager 4.0 and Router Software Version 10.0 are backward compatible with earlier versions of the router code. You can boot an IPX configuration that operates with an earlier version (for example, 8.10) on a router that has Version 10.0 software, and the software will update the configuration. You can then go into dynamic mode (or save the updated configuration and go into remote mode) and edit any of the new parameters. When you save the edited configuration, you're saving a Version 10.0 file.

In local mode, Site Manager will run IPX configurations from an earlier version using the Management Information Base (MIB) for that version instead of the MIB for Version 10.0. If you choose to continue using a router configuration that you configured under a software version earlier than 10.0 without updating it, you will not get the Version 10.0 features, and you must use the Version 8.10 guide *Customizing IPX Services* instead of this guide.

About the IPX Protocol

The Internet Packet Exchange protocol is the Novell, Inc., adaptation of the Xerox Network System (XNS) protocol. IPX has the following characteristics:

- It is a *connectionless datagram* delivery protocol. *Connectionless* means that it does not need a channel established for packet delivery. A *datagram* is a unit of data that contains all the addressing information required for it to be delivered to its destination. The path or route that one datagram follows to reach a destination is independent of the path or route that another datagram may follow to reach the same destination.
- It does not guarantee the delivery of packets. Higher-level protocols assume the responsibility for reliability. The higher-level protocols that IPX uses are described in the section "Handling Packets Associated with Upper-Layer Protocols."
- It uses the Internet Data Packet (IDP) format.

IPX is the network-layer routing protocol used in the NetWare environment. The primary tasks of IPX are addressing, routing, and switching information packets from one location to another on a network. The network interface card (NIC) in a client provides network node addressing. IPX defines the *internetwork* and *intranode* addressing as follows:

- Network numbers form the basis of the IPX *internetwork* addressing scheme for sending packets between network segments. Every network segment of an internetwork is assigned a unique network address by which routers forward packets to their final destination network. A network number in the NetWare environment consists of eight hexadecimal characters. In the following example, *0x* indicates that this is a hexadecimal number, and *n* is any hexadecimal character.

  0xnnnnnnnn

- Socket numbers are the basis for an IPX *intranode* address; that is, the address of individual entities within a node. They allow a process (for example, RIP or SAP) to distinguish itself to IPX. To be able to communicate on the network, the process must request a socket number. Any packets IPX receives addressed to that socket are then passed on to the process within the node.

The remainder of this chapter provides information about internetworking services that the Bay Networks router running IPX supports.

Supported LAN Circuits, WAN Circuits, and Frame Formats

You can choose a combination of physical circuits and data-link layer frame formats that are appropriate for the types of clients and applications on your network. Table 1-1 shows the types of LAN circuits and frame formats supported by Bay Networks routers running IPX.

Table 1-1. LAN Circuit and Frame Support for IPX Interfaces

Circuit Type	Frame Type — Novell Terminology	Frame Type — Bay Networks Terminology
Ethernet	ETHERNET_II ETHERNET_802.2 ETHERNET_802.3 ETHERNET_SNAP	ETHERNET LSAP NOVELL SNAP
TOKEN RING	TOKEN-RING TOKEN-RING_SNAP	LSAP SNAP
FDDI	N/A	LSAP SNAP

Table 1-2 shows the relationships between the types of WAN circuits, the WAN protocols, and the frame formats supported by Bay Networks routers running IPX.

Table 1-2. WAN Circuit and Frame Support for IPX Interfaces

Circuit Type	WAN Protocol	Frame Type — Bay Networks Terminology
Synchronous: —V.35 —RS-232/V.24 —RS-422/423 —X.21 —T1/Fractional T1 —E1/Fractional E1	These protocols apply to all these circuit types: —ATM —Frame Relay —PPP —SMDS —X.25 Point-to-Point —X.25 PDN —Bay Networks Point-to-Point	 SNAP SNAP PPP SNAP ETHERNET RFC 1356 ETHERNET

Table 1-2. WAN Circuit and Frame Support for IPX Interfaces

Circuit Type	WAN Protocol	Frame Type — Bay Networks Terminology
HSSI	ATM Frame Relay PPP SMDS Bay Networks Point-to-Point	SNAP SNAP PPP SNAP ETHERNET
ISDN	PPP	PPP

Refer to Chapter 3, "Enabling IPX Services," of this manual for information on selecting the appropriate frame format. Refer to *Configuring Routers* for instructions on configuring a physical LAN or WAN circuit.

Network-Level Services

A Bay Networks router running IPX provides the following network-level support:

- Dynamic routing of IPX packets
- Multiple IPX interfaces per circuit
- IPX over WAN media
- IPXWAN and IPXCP
- Routing Information Protocol (RIP and Unnumbered RIP)
- Service Advertising Protocol (SAP)
- Static Route support
- Default Route support
- Adjacent Host support
- Dial-on-Demand support

Dynamic routing occurs normally on any IPX interface; brief descriptions of the other supported capabilities follow.

Multiple IPX Interfaces per Circuit

You can use the multiple-encapsulation support feature of IPX to configure one or more IPX interfaces per physical circuit. The number of IPX logical interfaces you can configure on a circuit equals the number of unique frame formats available for that circuit type. (See Table 1-1 or Table 1-2 for details on circuit types and frame formats.)

For example, you can configure up to four IPX interfaces on a single Ethernet circuit, because the Bay Networks router supports four unique frame formats that are suitable for communication over an Ethernet LAN segment. To differentiate between IPX interfaces configured on the same physical circuit, the Bay Networks router uses the unique network address and frame format that you assign to each interface.

By supporting multiple IPX interfaces on a single physical circuit, a Bay Networks router can service clients on independent *logical* LANs that coexist on the same *physical* LAN segment.

In Figure 1-1, each client on the right side of the router has a different logical network address and uses a different encapsulation method. If all clients need to access Server 1, then only Interface 1 of the router needs to support all the different encapsulation methods and multiple logical network addresses for the workstations. Interface 2 of the router needs to support only the SNAP encapsulation method that Server 1 supports.

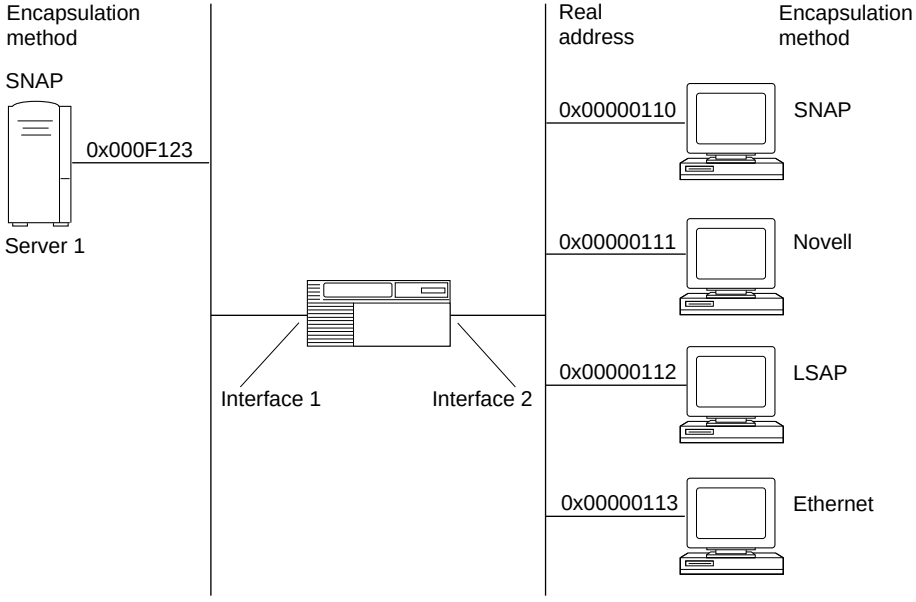

Figure 1-1. Multiple IPX Interfaces per Physical Circuit

Note: ***NetWare users —*** *If you are upgrading client and server stations on your network to Novell NetWare Version 4.x, you can use the multiple-interface-per-circuit capability to gradually migrate stations on the same network segment to NetWare Version 4.x (that is, from one logical network to another, independent logical network).*

For example, you can upgrade and migrate NetWare clients from a logical network that supports only Novell (802.3) encapsulated frames to a logical network that supports a more versatile Link Layer Service Access Point (LSAP) (802.2 frame type).

IPX over WAN Media

You can implement an IPX connection over any of the previously listed WAN media types. The choice of protocols depends on the type of connection and what you want the protocol to do.

The WAN protocol PPP uses the IPXCP protocol (RFC 1552). IPXCP supports the routing of IPX packets over wide-area links that support only the Point-to-Point Protocol. IPXCP is a data link protocol that is part of PPP. To enable IPXCP, you must first configure the interface to support PPP. For instructions on how to do this, refer to *Configuring PPP Services*.

For the Frame Relay and PPP WAN protocols, you can optionally run IPXWAN (RFC 1634).

Note: *You use IPXCP or IPXWAN when you want the routers to negotiate the options required for communication over the WAN link. Alternatively, you can explicitly specify the values for the WAN link without using either IPXCP or IPXWAN, as long as you ensure that what you configure at each end of the link is compatible.*

Using IPXCP and IPXWAN

Incorporating IPXCP and IPXWAN in the Bay Networks router provides the following benefits:

- Adherence to RFCs 1362 and 1634 IPXWAN protocols developed by Novell
- A common link negotiation method for WAN media (Frame Relay and PPP)
- Interoperability with other routing vendors (for example, Novell)
- A standardized means for tick-based routing over WAN media.

If you configure a local and a remote node to support both IPXCP and IPXWAN, IPXCP always runs first. After the router completes IPXCP negotiation, it discards all IPXCP-negotiated options, and IPXWAN runs.

Running IPXWAN over PPP

IPX uses PPP when operating over point-to-point synchronous networks. With PPP, establishing a connection means that the IPX Network Control Protocol (NCP), IPXCP, reaches the Open state.

PPP lets either side of a connection stop forwarding IPX packets if one end sends an IPXCP Terminate request. When a router detects this, it immediately reflects the lost connection in its routing information database.

Running IPXWAN over Frame Relay Permanent Virtual Circuits

Each IPX packet is encapsulated in a Frame Relay frame. When an interface is restarted, IPXWAN exchanges begin immediately over active, direct mode Frame Relay PVCs (those that have remained active before and after restart).

- When a router detects that a direct mode Frame Relay PVC has gone from an inactive to an active state, the connection is established, and IPXWAN packet exchange over this newly activated connection begins.
- When an active PVC becomes inactive, the router reflects the lost connection in its routing information database.

Note: *For IPX, you can use Frame Relay's direct, group, or hybrid mode. For IPXWAN, only direct mode is valid. In Frame Relay, direct mode is a point-to-point connection. Frame Relay group mode (or hybrid mode) involves a point-to-multipoint connection.*

Negotiating an IPXWAN Connection

Establishing an IPXWAN connection involves negotiating which router will be the primary link. Being the primary link does not imply any special privileges; it simply indicates which router is the requestor in the ensuing request/response exchanges. A router retains its role — primary or secondary — for the remainder of the IPXWAN exchanges. The following options are determined after successful negotiation by the IPXWAN protocol:

- WAN link delay used in tick-based routing across the WAN link
- Network number for the WAN link
- Routing protocol to be implemented over the WAN link

IPX Network Numbers

The examples that follow use these terms: *network number*, *Primary Network Number, Common Network Number,* and *router names*. These terms mean

- A *network number* is an identifier that uniquely designates the IPX network segment associated with an interface. The range of valid network numbers is 0x00000000 through 0xFFFFFFFD. Network number 0xFFFFFFFE is reserved for default routes. Refer to the description of default routes later in this chapter for more information on support for default routes and to Chapter 4 for information on configuring default route parameters.

- A *Primary Network Number* (PNN) is a string of up to 8 hexadecimal characters that specifies an IPX network number for IPXWAN (RFC1634-compliant) link negotiation on all slots. The value of the PNN determines whether the local or remote WAN interface serves as IPX primary link. The node with the highest PNN value becomes the IPX primary link. The range of valid PNNs is 0x00000001 through 0xFFFFFFFD.
- A *Common Network Number* (CNN) is an IPX network number that is available for assignment to the WAN link. The range of valid Common Network Numbers is 0x00000000 to 0xFFFFFFFD.
- A *router name* is a symbolic name that you assign to the router.

The next three sections apply only to IPXWAN interfaces.

Primary Network Number

Like Novell routers and servers, a Bay Networks router running IPX implements a global "internal network," to which you must assign a network number called the Primary Network Number (PNN) if you configure the IPXWAN protocol on any interface. IPXWAN requires the PNN to determine whether the local or the remote router on a WAN link serves as the primary or secondary during the IPXWAN negotiations. The router with the higher PNN serves as the primary link.

You enter the Primary Network Number in the IPX Global Parameters window of the Configuration Manager tool. Refer to Chapter 4 for more information on how to access the IPX Global Parameters window.

Common Network Number

The Common Network Number (CNN) is an IPX network number that is available for assignment to the WAN link. You specify a CNN that IPXWAN, running on the interface, can assign to the WAN link. To assign its CNN, the router must serve as the primary link during the IPXWAN negotiations. To specify a CNN, use the IPXWAN Common Network Number Parameter in the Configuration Manager IPX Interfaces window. Refer to Chapter 4 for more information on how to access this window.

All values between 0x00000000 and 0xFFFFFFFD, inclusive, are valid CNN values. Never use the values 0xFFFFFFFE or 0xFFFFFFFF as CNN values; these values are reserved.

Router Names

Every IPX router can have a router name. During IPXWAN negotiations, the local and remote routers provide each other with their respective router names. Once the link is established, the name lets a router know whom it is connected to. Router names are particularly helpful for network management purposes. A symbolic name, such as “printserv,” has more meaning than just a string of digits.

The router name can be up to 47 characters long and can contain the characters A through Z, a through z, 0 through 9, and the special characters underscore (_), hyphen (-), slash (/), and “at” sign (@). Some valid names include

- AAaabbBBxxXXXS/1234
- myrouter@first_floor
- Chicago_office

Sample IPXCP and IPXWAN Configurations

Figure 1-2 shows a local router communicating with a remote router using IPXCP over PPP, and the same local router communicating with a remote router using IPXWAN over Frame Relay.

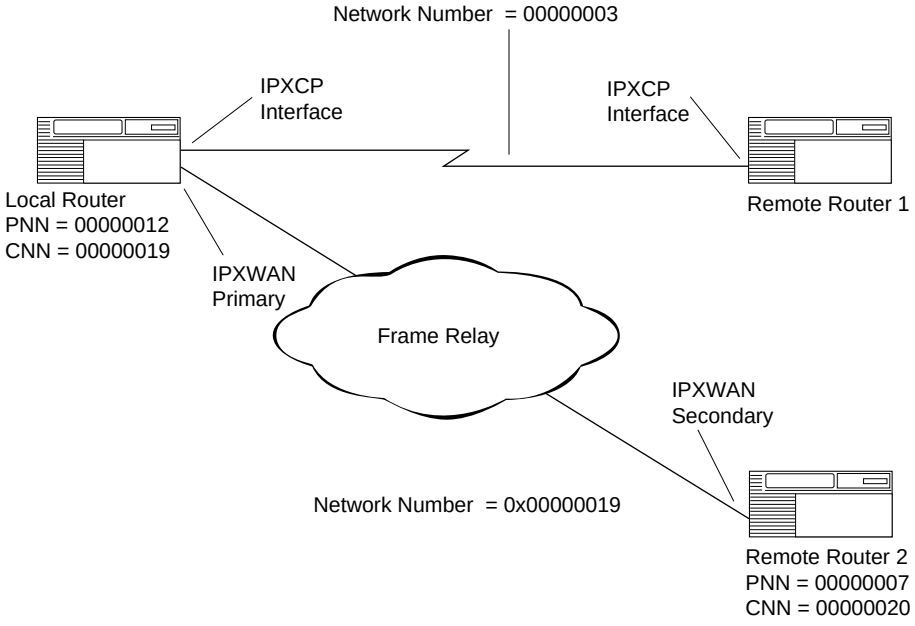

Figure 1-2. IPXCP and IPXWAN Configurations

IPXCP Link Negotiation

In Figure 1-2, the local router and Remote Router 1, both configured for IPXCP, negotiate a connection at the data link layer. Once the options are successfully negotiated, the IPXCP interfaces in both the local router and Remote Router 1 must agree on a unique network number. When you initially configure an IPXCP interface, you assign an IPX network number to that interface. The routers select the higher of the two IPX network numbers. See *Configuring PPP Services* for instructions on configuring the IPX network number for an IPXCP interface.

Note: *For PPP communication between a Bay Networks Version 7, 8, 9, or 10 IPX router and a Bay Networks Version 5 IPX router (or any other vendor's router that does not support IPXCP negotiations), you must statically configure the network number of the IPX interface on both routers.*

IPXWAN Link Negotiation

The local router and Remote Router 2 are both configured for IPXWAN. When you initially configure an IPXWAN interface, you assign a PNN to the router. The router with the highest PNN becomes the primary link during IPXWAN negotiations on that WAN link.

In Figure 1-2, the local router (PNN=00000012) is the primary router, and Remote Router 2 (PNN=00000007) is the secondary router. During the IPXWAN negotiations, both routers negotiate their link options. If successful, the CNN configured for the interface on the primary router becomes the IPX network number for the WAN link.

Once the IPXWAN negotiations are successful on the WAN link, each router connected on the link can build its routing/forwarding tables.

IPXWAN and IPXCP Link Configurations

Table 1-3 shows the various WAN protocol configurations likely to exist within local and remote IPX router interfaces. Find the configuration that applies to your situation, as indicated in the table, and read the corresponding description that follows.

Table 1-3. Configuration Table for IPX Over WAN Media

Local IPX Interface	Remote IPX Interface			
	IPXWAN with IPXCP	**IPXWAN but not IPXCP**	**PPP with IPXCP; no IPXWAN**	**PPP without IPXCP; no IPXWAN**
IPXWAN with IPXCP	Configuration 1	Configuration 2	Configuration 3	Configuration 4*
IPXWAN but not IPXCP	Configuration 2	Configuration 2	Configuration 4	Configuration 4
PPP with IPXCP; no IPXWAN	Configuration 3	Configuration 4	Configuration 3	Configuration 4
PPP without IPXCP; no IPXWAN	Configuration 4*	Configuration 4	Configuration 4	Configuration 4

* Bay Networks 9.00 to Bay Networks Series 5.*x* IPX Router Compatibility

Configuration 1 (IPXWAN with IPXCP on Both Interfaces)

In this configuration, IPXWAN defers to IPXCP for link negotiation.

- IPXWAN negotiation supersedes IPXCP negotiation, regardless of whether IPXCP negotiation succeeds.
- If IPXWAN negotiates successfully, the IPX interface becomes active. If IPXWAN negotiation fails, the IPX interface cannot become active.

Configuration Guidelines — Configuration 1

- IPXCP — Use the value zero for the IPX network number when configuring the local and remote Point-to-Point Protocol interface.
- IPXWAN — Use a unique router name and Primary Network Number in the IPX Global Parameters window when configuring the local routers.

You must enable IPXWAN on the interface. You must also enter a unique Common Network Number for the IPX interface you just configured, except that the CNN can be zero when Unnumbered RIP is configured on both interfaces.

Configuration 2 (IPXWAN on Both Interfaces)

In this configuration, IPXWAN exclusively negotiates an IPX network number for the link.

- If IPXWAN negotiates successfully, the IPX interface becomes active.
- If IPXWAN negotiation fails, the IPX interface cannot become active unless both sides are configured with a zero network number.

Configuration Guidelines — Configuration 2

- IPXCP — No configuration requirements.
- IPXWAN — Use a unique router name and PNN in the IPX Global Parameters window when configuring the local and remote routers.

You must enable IPXWAN on the interface. You must also enter a unique Common Network Number for the IPX interface you just configured, except that the CNN can be zero when Unnumbered RIP is configured on both interfaces.

Configuration 3 (Only IPXCP on Both Interfaces)

In this configuration, IPXCP exclusively negotiates an IPX network number for the link.

- If IPXCP successfully negotiates the number, the IPX interface becomes active on the link.
- If IPXCP fails to negotiate a number, the IPX interface cannot become active.

Configuration Guidelines — Configuration 3

- IPXCP — Use any valid value for the IPX network number when configuring the local or remote PPP interface.
- IPXWAN — No configuration requirements.

Configuration 4

In this configuration, the lower layer has no means of negotiating an IPX network number for the link. For this reason, you must manually configure the network number of the local and remote IPX interfaces to the same value.

Handling Packets Associated with Upper-Layer Protocols

The router encapsulates, within the data field of an IPX packet, any packets associated with Novell's upper-layer protocols. The structure of a packet, as well as the source and destination socket numbers contained in that packet, identify the protocol type associated with that packet; for example, Service Advertising Protocol and Routing Information Protocol. The upper layer services are

- The Novell Service Advertising Protocol, which provides a means for servers to advertise their services to routers and other servers.
- The Novell implementation of the Routing Information Protocol, which provides workstations and routers with a means for exchanging information dynamically. This information lets routers in the network establish a best or minimum-delay route to each destination network.

Bay Networks router software lets you select the basis on which an IPX router makes its routing decisions — on the number of *ticks* or the number of *hops*

required to reach a given destination network. The IPX routing software also provides the following services over LAN and WAN media:

- Multipath routing and load sharing
- Split Horizon capability
- NetBIOS (Network Basic Input-Output System) all-networks-broadcast packets (Type 20 packets)
- Source routing and endstation support
- IPX ping capability

The following sections describe how Bay Networks routers support these services.

Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) enables workstations and routers to exchange route information and to establish the route to each network with the fewest hops and shortest delay.

Each IPX router maintains a route table. The route table contains the following information about every network in the IPX network topology:

- The network address.
- The number of ticks (units of delay time) to that network. (A tick is equal to about $1/18^{th}$ of a second. The number of ticks to a network is the *tick cost* for that route. More information on this topic follows in the section "Routing Methods" in this chapter, and in Chapter 4.)
- The number of hops to that network. (A hop is an adjacent router; the number of hops is equal to the number of adjacent routers that a packet must traverse to reach another network segment.)
- The address of the next-hop node to which the local router forwards packets on their way to another destination network.

Routers maintain route tables by exchanging RIP request and response packets. A RIP request packet specifies the destination network. A RIP request packet can be

- A general request broadcast by a router to retrieve the fastest route to all known networks on an internetwork. The value 0xFFFFFFFF in the network address field indicates that the packet is a general request.

- A specific request broadcast by a workstation or router to determine the fastest route to a particular network. One or more network addresses (excluding an address of all Fs) in the network address field indicates that the packet is a specific request.

Routers at the destination network issue RIP response packets. RIP response packets contain the network number and the number of hops and ticks required to get to the network. A RIP response can be one of the following types:

- A response to a request.
- An informational broadcast from a router issued at regular intervals (by default, every 60 seconds).
- An informational broadcast when a change occurs in the routing table. Examples of changes in the routing table are tick or hop changes, timing out of routes, and the addition of routes to networks to the table.
- An informational broadcast when an interface initializes or performs an orderly shutdown procedure.

Each RIP packet can contain up to 50 route updates. To reduce traffic, RIP broadcasts are limited to a router's immediate segments and are not forwarded by receiving routers.

Note: *The IPX router learns WAN addresses from RIP and SAP broadcasts received over WANs (Frame Relay, SMDS, ATM). The router stores IPX address/WAN address pairs for future use as next-hop destinations.*

If RIP is not configured for a WAN interface, you must configure adjacent hosts for all transmission paths to nodes adjacent to Frame Relay, ATM, or SMDS circuits when you configure an IPX interface. You must then configure static routes that use the adjacent hosts to reach next-hop routers. Refer to the descriptions of adjacent hosts and static routes in this chapter for more information on these features.

The IPX router lets you enable the RIP listen and supply functions for each IPX interface. When you enable the listen function, the IPX router learns routes received in RIP updates from neighboring routers. When you enable the supply function, the IPX router transmits RIP periodic updates to routers in adjacent networks.

IPX Route Filters

You can apply filters to shield the view of networks and route paths from users on different network segments. As with SAP filters (described earlier in this chapter and in Chapter 4), you can configure route filters on individual router interfaces as inbound, outbound, or both for both local- and wide-area links.

Route filters give you greater control over the routing of IPX packets from one area of a NetWare internetwork to another. This helps maximize the use of the available bandwidth throughout the IPX internetwork, and helps improve network security by shielding a user's view of other networks.

You define IPX route filters using the network number field in the IPX RIP packet header. In effect, the filter tells the router to perform some action related to the network (advertise, accept, or suppress route information) when the network number matches the filter. The filter is matched against the network number in the RIP packet (inbound) or in the routing table (outbound). The action parameter that you define for the filter determines whether the router advertises, accepts, or suppresses RIP packets from routers that match the filter pattern.

If an inbound packet is not filtered, or if an inbound RIP packet matches the filter and if the action is accept, IPX processes the packet to see if it's the best route before putting this route into the routing table. See the description of using route filters in Chapter 4 for detailed information on how to set up and use IPX route filters.

Configuring RIP and SAP Broadcast Timers

A Bay Networks router running IPX lets you control the frequency of RIP and SAP update packet transmissions over both local-and wide-area links. RIP and SAP transmissions provide the following benefits:

- You spend less time manually configuring changes to static services and service routes across your network.
- You reduce the cost of administering Bay Networks routers installed across your network, compared to the cost of building static routes or static services tables.
- You allow a router to respond to changes in services and routes offered on the network.

- You enable users to have more accurate, up-to-date information on services and service routes offered on the network.

However, periodic RIP and SAP transmissions mean

- Less bandwidth is available for user data. Consequently, user data transmissions take longer, thereby increasing WAN line costs.
- You sacrifice some level of manual control over services and routes made available to network users. Your particular networking environment may require a higher degree of manual control over information on services and service routes offered to users on your network.

You can adjust the frequency of RIP and SAP update packet transmissions by specifying the Update Interval parameter (in seconds) on the IPX RIP Circuit window or the IPX SAP Circuit window (respectively) for the particular circuit. The higher the number you enter, the less frequent the transmissions. If you enter zero, no periodic RIP or SAP updates are sent out the IPX interface of the router. However, RIP and SAP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards. The default interval is 60 seconds. See Chapter 4 for instructions on configuring these parameters.

Eliminating periodic RIP and SAP updates provides the following benefits:

- Reduced RIP and SAP overhead on your network
- Increased bandwidth available for user data
- Reduced WAN line costs for packet transmission
- Increased manual control over network services and routes

However, not having periodic RIP and SAP transmissions means

- A slower response time of the network to changes in network services and routes
- An increase in the time and cost of administering changes to services and service routes made available through Bay networks routers on your network

RIP and SAP timer settings should be the same on both sides of the WAN. Refer to the sections “Configuring RIP Timers” and Configuring SAP Timers” in this chapter for more detailed information.

Routing Methods

To specify a method for making IPX "best-route" decisions for all slots, based on time delays (ticks) incurred or hops encountered for packet delivery, use the Routing Method parameter on the Edit IPX Advanced Global Parameters window. Refer to Chapter 4 for instructions on using this parameter.

The router can assess the time delay in one of the following ways:

- *Number of RIP timer ticks* — the amount of time, expressed in ticks, that a packet requires to reach another network segment. (Each RIP timer tick equals about $1/18^{th}$ of a second. The maximum configurable number of ticks is 65,534 ticks, multiplied by $1/18^{th}$ of a second = 3600 seconds, or 60 minutes.
- *Number of hops* — the number of router hops a packet must traverse to reach a network segment. The maximum number of hops is 15.

We recommend using the default (tick-based) method.

Configuring Interface Costs

You can set the cost (number of ticks or hops) for an interface using the Cost parameter on the Edit IPX Advanced Global Parameters window. The value you enter depends on whether you selected hops or ticks for the RIP Method parameter. For more information about specifying the Cost parameter, refer to Chapter 4.

By configuring an interface's cost you can select the route you want to use, rather than letting the network select the route. For example, two routes go to the same destination. Route A has a tick cost of 2; Route B has a tick cost of 3. Because Route A has the lower tick cost, the network selects it as the "best route" to the destination. If you want traffic to go over Route B, you can set the tick cost of Route A to 4, which then forces traffic to go over Route B.

Using configurable RIP interface tick values, IPX routing decisions can be based on tick values that you define. This allows the implementation of tick-based routing over non-IPX WAN links (for example, HDLC encapsulation), letting you optimize IPX network performance.

In Figure 1-3, for example, traffic generated by End System 1 (ES1) on Network A is directed to the IPX Server ES2 on Network B over Interface 2 (route of least tick delay, per RIP specification). However, other protocols such as IP, AppleTalk

2, and OSI will most likely select this route as the least-cost path between Network A and Network B, as well. Consequently, traffic congestion over this route may preclude it from being the most efficient path between these two network segments.

By implementing the Configurable RIP Interface Tick parameter, Interface 1 on Router 1 can be assigned a lower tick value than Interface 2, so that IPX traffic is routed through Interface 1. This lets you maximize IPX internetwork performance between Networks A and B, even though it traverses two T1 lines instead of one.

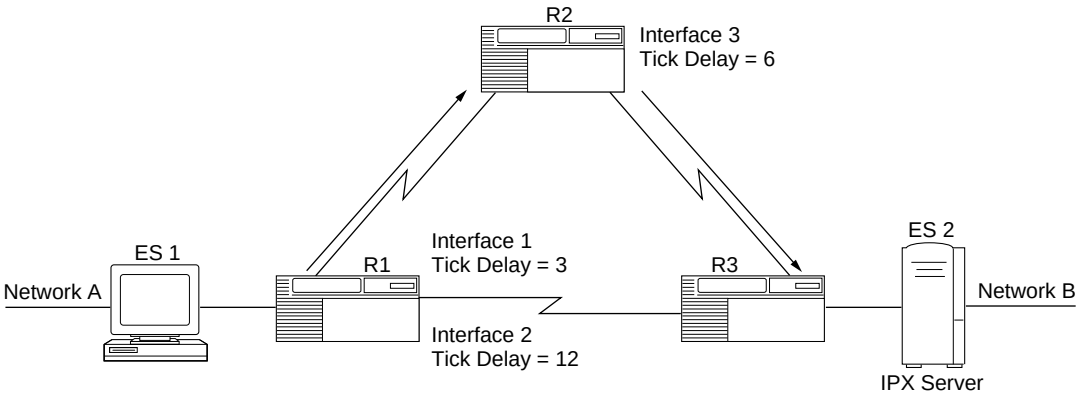

Figure 1-3. IPX Configurable RIP Interface Cost

Configurable RIP Timers

You can extend the standard 60-second IPX periodic RIP advertisement interval for RIP timers by multiples of the update interval that you specify. You configure the interval by specifying the value of the Update Interval parameter, and the multiplier by specifying the Age Multiplier parameter. Refer to Chapter 4 for details on how to configure these parameters.

Configuring RIP timers can reduce IPX RIP overhead and enhance bandwidth availability. Furthermore, you can eliminate periodic RIP advertisements by setting the configurable RIP timer to zero; thus, only RIP updates triggered by changes in the internetwork topology will be propagated.

To ensure proper RIP operation, all configurable RIP timers must be set at equal advertisement intervals on all Bay Networks router interfaces attached to common

IPX network segments. To alleviate the unnecessary timing out (purging) of RIP entries, the configurable RIP timers feature also automatically extends an entry's RIP age-out time to three times the value of the RIP advertisement setting of the interface on which the entry was learned. Standard RIP operation purges any RIP table entry for which route information is not received (in a RIP update) after 180 seconds (three times the standard 60-second RIP advertisement interval).

Note: *While you can set configurable RIP timers on any Bay Networks router interface, do not use them on LAN interfaces, because IPX servers do not allow configuration of update timers (with internal routers). As a result, IPX servers will purge RIP entries after 180 seconds if they have not received any updates within the standard 60-second interval.*

For example, in Figure 1-4, if Router R1 is configured to issue periodic RIP advertisements every 240 seconds over Interface 1 and Router R2 is configured to issue advertisements per the IPX standard (every 60 seconds) over Interface 2, then Router R2 will purge RIP entries learned through Interface 2 every 180 seconds and reinstate them 60 seconds later when it receives a periodic RIP advertisement from Router R1. More critically, Router R2 will issue triggered RIP updates through Interface 3, propagating these unnecessary changes throughout the internetwork behind Router R2.

Setting the configurable RIP timers at 240 seconds on both Interface 1 on Router R1 and Interface 2 on Router R2 ensures proper RIP operation, because RIP entries are not purged unless an update for a particular entry is not received within a 720-second interval (3 * 240 seconds).

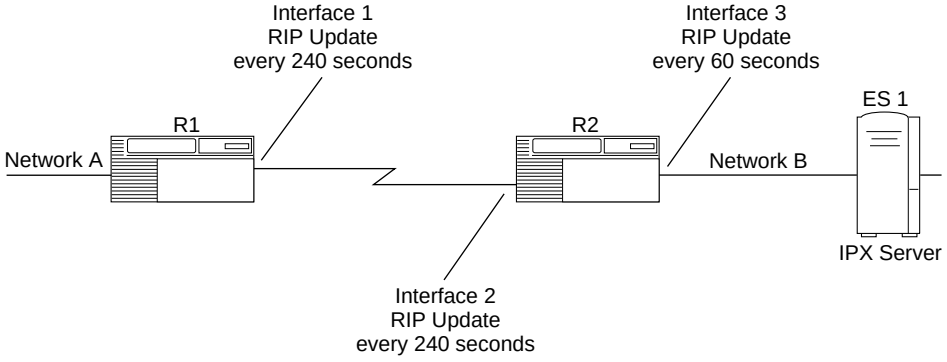

Figure 1-4. IPX Configurable RIP Timers

Taking into account the fact that IPX Server ES1 (with an internal router) on Network B expects periodic RIP advertisements every 60 seconds, Router R2 continues to issue RIP advertisements out its LAN interface (Interface 3) per the IPX specification, reconciling the fact that periodic RIP advertisements through Interface 1 are received every 240 seconds.

Multipath Routing and Load sharing

You can include multiple next-hop destinations as active routes to a destination network. The IPX router can find out about multiple paths by either RIP packets or statically configured routes.

The router can forward packets to the multiple next-hop nodes concurrently by multiplexing frame transmissions over the multiple equal-cost paths in a cyclic sequence. This is referred to as *IPX multipath* or *IPX load sharing*.

Multipath Routing

Multipath is a “round-robin” or cyclic multiplexing mechanism. When multiple least-cost paths of equal tick delay and hop count exist between IPX source and destination networks, standard RIP operation uses only one of these routes. The multipath feature takes advantage of these multiple equal-cost routes and distributes the packet load among them, balancing the IPX traffic across these routes and maximizing internetwork performance. When you enable multipath routing, the IPX router diverts individual, consecutive frames destined for the same target network to separate IPX interfaces and their associated physical circuits. (Figure 1-5.)

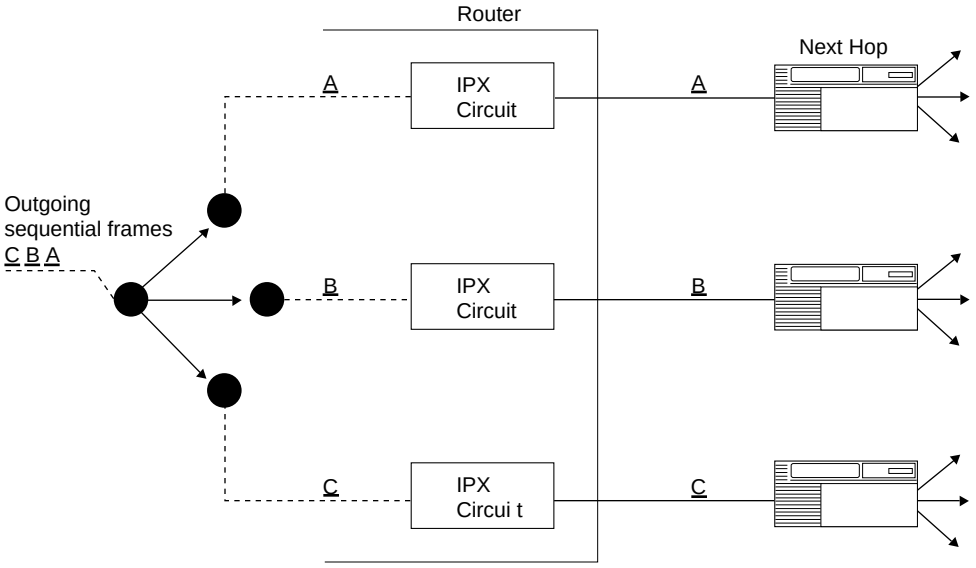

Figure 1-5. IPX Multipath

Because the IPX interfaces have duplex functionality, the router can also use multipath to collect frames received from separate IPX interfaces. The router operates this cyclic mechanism at a bandwidth significantly greater than a single IPX interface and its supporting physical circuit can support. The result is that IPX frames flow over multiple parallel LAN or WAN routes concurrently, in effect, aggregating the bandwidth supported by the parallel routes. Each line shares $1/n^{th}$ of the total load (where *n* is the number of equal-cost parallel routes or paths to the destination network).

You set the maximum number of paths (up to five) by means of the Maximum Path parameter on the Edit IPX Advanced Global Parameters window. Refer to Chapter 4 for instructions on setting this parameter. Any setting greater than 1 engages the multipath mechanism. Figure 1-6 is an example of equal, least-cost, parallel routes used in IPX multipath routing.

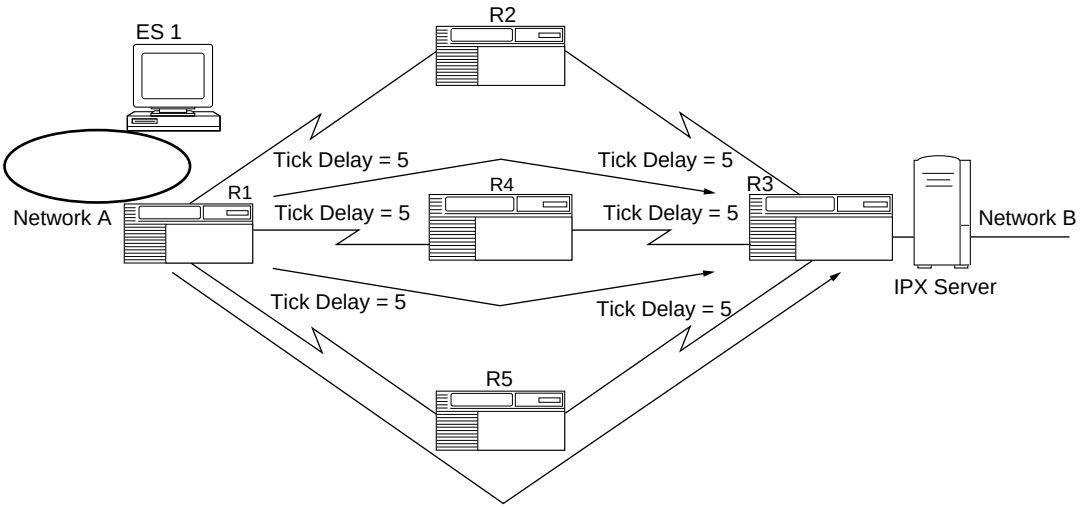

Figure 1-6. IPX Multipath Routing — Equal Least-Cost Routes

Because of the round-robin algorithm, IPX packets that belong to the same data stream may require resequencing at their ultimate destination. Therefore, higher-layer protocols such as SPX must be used in both source and destination IPX routers to provide packet resequencing. To derive maximum benefit from this feature, the source and destination nodes should support burst-mode operation.

Load Redistribution and Rerouting

If the router with multipath enabled detects a failure, it temporarily redistributes the IPX traffic among the remaining active original least-cost routes. When the router learns (through RIP packets) of the existence of an alternative least-cost route, or when the failed route returns, IPX multipath returns to its original IPX traffic distribution.

Multipath Route Precedence/Priority

The multipath mechanism generally uses the best path first. However, when two equal-cost paths exist, multipath uses the following priority scheme for route selection:

1. Routes learned via RIP
2. Statically configured routes
3. Direct routes (paths to other routers on a segment directly attached to the local router)

Multipath Configurations

You can establish equal-cost multipath routes over LAN or WAN segments to support IPX traffic between routers, and between routers and servers. The slower the interconnecting LAN or WAN links, the more difference using multipath will make in client/server throughput.

Multiline Circuits

The multiline circuits feature allows a single circuit to be composed of up to 16 individual synchronous network data paths. Multiline circuits support provides a level of redundancy not available through conventional single-line circuit configurations. The multiline circuits feature ensures routing circuit availability in the event of a single data path failure.

Equally important, the multiline circuits feature provides increased bandwidth between two sites without the circuit management complexities associated with multiple circuits. Once you've configured and enabled the circuit, the use of multiple data paths to form a single circuit is transparent to both network management and the end-user community.

Multiline circuits provide the following methods for transmitting traffic over their data paths:

- Address-based data path selection
- Random data path selection

Address-based data path selection determines the path a packet traverses based on its source and destination addresses. Once a path has been established for a given address pair, subsequent packets will follow the same path. This ensures that

packets will be received in the order in which they were sent. This is essential for protocols that cannot tolerate receiving packets out of order.

Random data path selection determines the path a packet traverses based on a randomly assigned number that corresponds to a particular data path of the multiline circuit. This algorithm avoids congestion by providing even distribution across multiple data paths. Unlike address-based selection, random data path selection does not guarantee the sequence of packets as they are received at their destination. Consequently, random data path selection is intended for use with protocols whose upper layers provide resequencing techniques.

Note: *For Bay Networks software Version 7.60 and later, support of multiline circuits is compatible with the Version 5.x "Circuit Groups" feature, except that Version 7.60 and later software does not support LAN media multiline circuits grouping. Multiline circuits can be configured using only synchronous interfaces data paths, including HSSI. All data paths must incorporate the same encapsulation method, Maximum Transfer Unit (MTU), and effective bandwidth.*

The differences between multiline circuits and IPX multipath are the following:

- Multiline circuits operate across point-to-point links between two Bay Networks routers, while IPX multipath operates across a random topology (both LAN and WAN)
- Multiline is protocol-independent, while IPX multipath is IPX-based
- Multiline circuits require WAN links of equal bandwidth on which to distribute IPX traffic, while IPX multipath supports links of varying speeds
- Multiline circuits do not support the adoption of alternative links when WAN links fail

Configurable Split Horizon

The Split Horizon algorithm is part of the Novell specification for the IPX protocol. Its purpose is to prevent circular routes and reduce network traffic. The Bay Networks implementation of Split Horizon excludes RIPs and SAPs learned from a neighbor when forwarding RIP and SAP updates to that neighbor. Split Horizon is enabled by default for each interface. You can enable or disable Split Horizon when you configure the IPX RIP Circuit in the Configuration Manager.

Fully Meshed Networks

A fully meshed network is a WAN in which all nodes have a logically direct connection to each other. Figure 1-7 shows a sample fully meshed network with split horizon enabled.

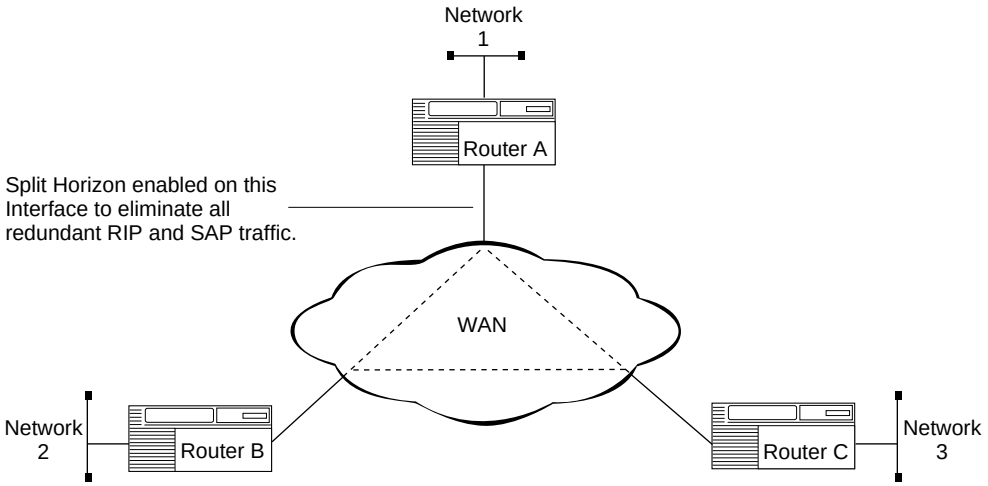

Figure 1-7. Split Horizon Enabled in a Fully Meshed Network

Nonfully Meshed Networks

A nonfully meshed network is a WAN in which one or more nodes do not have logically direct connections to all other nodes. In a star or nonfully meshed Frame Relay or X.25 PDN topology, you may need to disable Split Horizon on certain interfaces so the routers can learn about other networks.

Caution: *We advise you not to disable Split Horizon unless it is absolutely necessary. Doing so can result in a significant increase in network traffic.*

Figure 1-8 shows a sample nonfully meshed network with Split Horizon disabled.

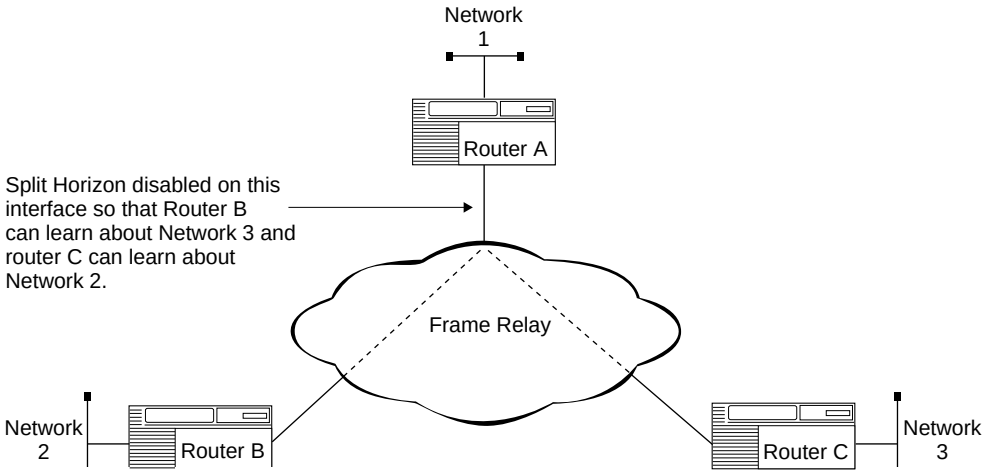

Figure 1-8. Split Horizon Disabled in a Nonfully Meshed Network

Disabling IPX Split Horizon allows the dissemination of a complete impression of IPX internetworks (routes and services) over nonfully meshed Frame Relay and SMDS topologies. As such, Router A propagates RIP and SAP packets pertaining to Router B to Router C, and vice versa. As a result, endstations on Network 2 can learn about Network 3, and endstations on Network 3 can learn about Network 2.

Static Route Support

A static route specifies a transmission path between networks.

The static route feature lets you manually define an IPX route to a destination network. Static routes specify the next hop in the transmission path a datagram must follow, based on the datagram's destination address. You configure a static route when you want to restrict the paths that packets can follow. A Bay Networks router running IPX lets you configure static routes on each logical IPX interface.

Using static routes is most valuable over wide-area links, where bandwidth is at a premium. Static route support also enhances internetwork security because it can be implemented so that traffic across specific IPX networks is restricted, protecting sensitive internetwork resources.

Static route support for IPX can do the following:

- Direct all IPX traffic not destined for this network to an adjacent host. The adjacent host may be the actual destination, or it may be the next hop to the eventual destination network. See the following section on adjacent host support for more information about adjacent hosts.
- Reduce routing traffic by disabling the RIP supply function on all or a subset of attached interfaces that are configured with static routes.
- Provide security by eliminating all dynamic routing capabilities and all RIP supply and listen activities over an IPX interface.

You should configure static routes and disable IPX RIP and SAP advertisements when implementing dial-on-demand routing over a wide-area link. IPX RIP and SAP advertisements force dial-on-demand connections to be continuously established, which prevents user-defined dial-on-demand expiration time limits from being reached. Refer to the description of the dial-on-demand feature later in this chapter for details on using this feature.

Unlike routes learned through RIP, static routes remain in the route tables until you delete them. Static routes have priority over RIP-learned routes if both routes have the same cost.

If you do not have the RIP listen functions enabled, the local network will not learn about new routes on the network, route changes, or deleted routes.

Static route support lets you identify the next interface and next router in the path toward a destination network. Once you configure a static route for an interface, the router advertises that route in its usual RIP broadcasts.

For example, in Figure 1-9, to establish a static route between IPX Network A and IPX Network B, through Interface 1 on Router R1, a static route must be established from Router R1 to Router R2. The static route entry in Router R1 directs any traffic destined for Network B through Interface 1 to Router R2. In turn, the static entry in Router R2 directs any traffic destined for Network B through Interface 3 to Router R3, and thus to Network B.

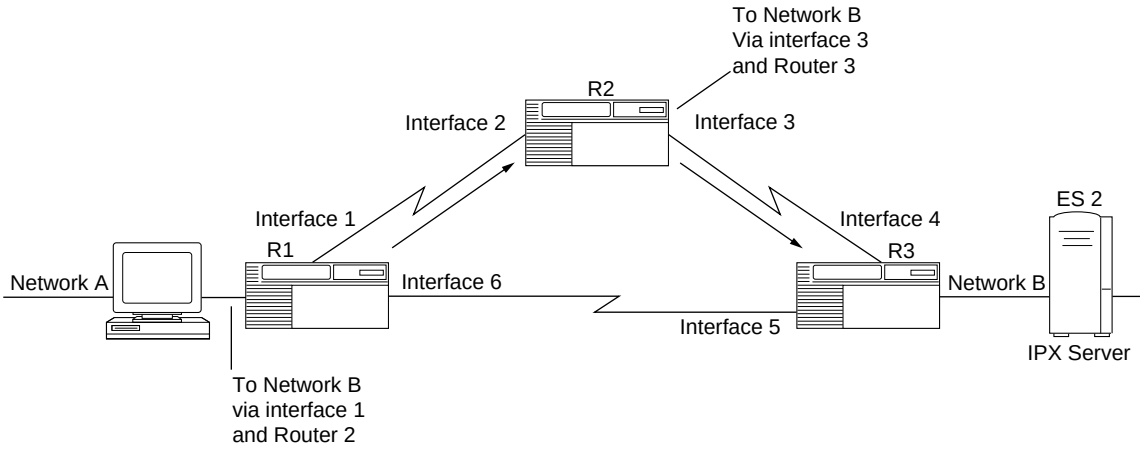

Figure 1-9. IPX Static Routes

Static routes have priority over RIP-learned routes with the same cost, so if the connection between routers R1 and R3 has the same or greater cost, the packet will travel over the static route from Router R1 to Router R2 to Router R3. If a connection used by the static route fails (and if Router R1 has the listen function enabled), Router R1 will learn of an alternative route between Network A and Network B and attempt to send the packet over that connection.

Default Route Support

A default route is a special case of a static route. A default route specifies a transmission path for an IPX router to use when it receives an IPX packet that does not contain a known IPX address within the IPX protocol header. You can configure and advertise default routes on an interface basis. Configuring a default route gives you greater control over what happens to packets transmitted over your network. If you do not configure a default route, an IPX router will drop a packet whose destination address is unknown.

Default routing provides a basic level of route aggregation in an IPX network. When packets need to be forwarded to another network not known to the router, they are forwarded to the default route. By default, default routing is disabled. You control the propagation and learning of default routes on an interface basis. Refer to Chapter 4 for a description of how to configure the parameters necessary to enable or disable default routing.

Adjacent Host Support

An adjacent host is a network device that is directly reachable without an intermediate hop; that is, a device that is directly attached to the same network as the router.

On a LAN, the node ID in the IPX header is the data link address of the destination host for the packet. In the case of WAN data link protocols, the node ID defined is not the data link address. You can define an adjacent host to map the node ID of the IPX host to the required data link address.

When you set up an adjacent host, you configure the adjacent host's host ID and a DLCI or WAN address. The DLCI/WAN address parameter identifies a virtual circuit when you configure a static adjacent host in a Frame Relay, ATM, or SMDS network. (ATM and SMDS don't use DLCI.) The router uses this information to build its adjacent host mapping table. Refer to Chapter 4 for more information on how to configure adjacent host parameters.

Note: *You don't need to configure adjacent hosts when running over PPP or Direct Mode Frame Relay.*

Under normal IPX operation, routers connected to Frame Relay, SMDS, or ATM networks learn DLCI (Frame Relay) and ATM and SMDS address information from IPX RIP packets. The router uses this information to build DLCI or SMDS address-to-IPX address mappings. However, IPX RIP overhead may cause excessive congestion over these networks. Adjacent hosts eliminate the need for periodic RIP advertisements by supporting the static configuration of DLCI or SMDS address-to-IPX mappings.

You should configure IPX adjacent hosts only when you are running IPX over Frame Relay (Group Mode), ATM, or SMDS and you do not have RIP configured on the IPX interface.

Once you configure an adjacent host and static routes, you can then disable RIP. This reduces the amount of RIP overhead on your network and increases the amount of bandwidth available for user data.

Figure 1-10 shows two routers, R1 and R2, directly connected to the same Frame Relay SVC network segment and configured as adjacent hosts with a static route

between them. Network C is connected to Network B through Router R3, but has no direct connection to Network A.

A static route exists from Interface 2 on Router R2 to Network A, and another static route exists from Interface 1 on Router R1 to Network C. The objective is to transport IPX packets from Network A to Network C.

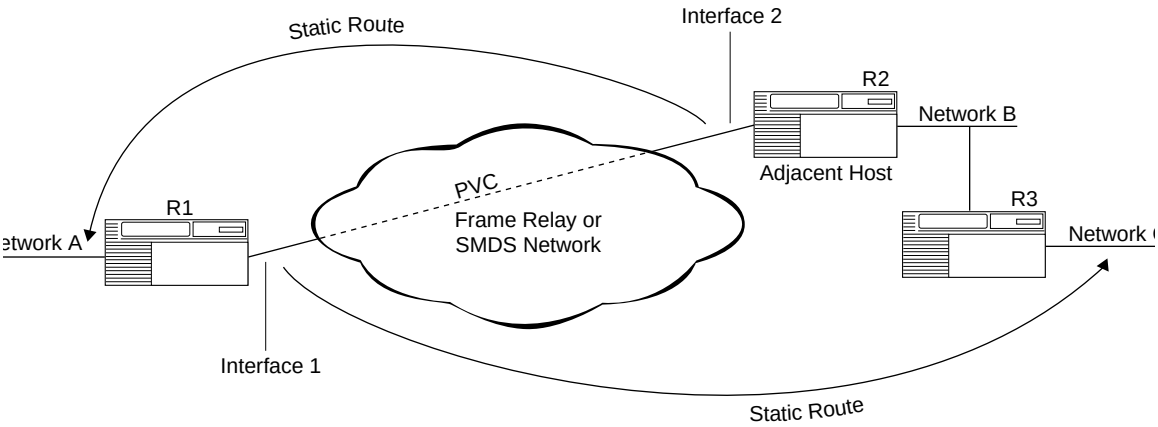

Figure 1-10. Using IPX Adjacent Hosts to Reduce Manual Configuration

Here's what happens:

1. As before, Router R1 consults its adjacent hosts table to map the node ID of the next-hop (Router R2, Interface 2) to the correct DLCI address.
2. Router R1 sends all IPX traffic destined for Network C (the target network) through the Frame Relay SVC (the next-hop network) to Router R2 (next-hop).
3. When a packet arrives, Router R2 consults its RIP table and dynamically routes the packet to its destination (Network C).

Service Advertising Protocol (SAP)

NetWare network services use the Service Advertising Protocol to inform clients of their presence. NetWare services use the SAP identification broadcasting services to tell clients their name, type, and IPX address. The IPX address in a broadcast identifies a server's location in terms of network, host, and socket.

NetWare Directory Services (NDS) and SAP

Networks that implement NetWare 4.*x* use the NetWare Directory Services (NDS) to advertise services. NDS is a globally distributed network database that replaces the bindery used in NetWare versions earlier than 4.0. Workstations locate services by querying an NDS server. NDS maintains information about all network resources (users, groups, servers, file volumes, printers, and so on) in a hierarchical tree structure. Network resources can be organized in the tree independent of their physical location. Thus, network users can access any network resource they have rights to without having to know the exact location of the resource.

With NDS, users no longer need to log in or attach to specific servers. Instead, users can log in to the network and get access to all authorized network resources. NDS is compatible with bindery-based versions of NetWare through the bindery emulation feature of NDS.

The NDS server distributes the service information using direct unicast-based protocols instead of using broadcast-based SAP. Therefore, the use of SAP in an NDS network is greatly reduced. Even in a network that includes only NetWare 4.0 servers, however, clients still use SAP to locate the nearest NDS server at startup.

SAP and the NetWare Bindery (NetWare 3.*x* and Earlier)

Novell IPX routers running NetWare versions earlier than 4.0 maintain a database called a *bindery.* The bindery includes information such as server type, IPX address, hop count, the interface to the server, a timer value for table entries, and a list of clients. If an entry in a bindery reaches its configured maximum age without being refreshed (timer resets to zero), the router deletes the entry from that bindery.

Bay Networks routers implement a similar structure (a global services table) for these services. Each time an IPX router receives a SAP packet, it compares the packet's contents to the contents of its SAP services table. If the SAP services table already contains information about a specific service, the router simply refreshes the age timer for that entry. If the SAP services table does *not* contain information about the service, and a route exists to the service, the router adds a new entry to the services table and advertises the new service to all connected networks (except the one on which it was received).

Clients use SAP to request information about network services. Client information requests are nearest-service queries, which seek information on the closest service of a specified type. Every IPX server and IPX router on the internetwork learns about all other IPX servers and services through the propagation of bindery information or services table information.

By default, each SAP packet can contain up to seven Service Advertising updates. This number is configurable, but it's constrained by the Maximum Transmission Unit of the outbound interface.

For a list of common service types, refer to Appendix A of this manual.

Configurable SAP Timers

Configurable SAP timers are similar in function to configurable RIP timers, except that one pertains to SAP advertisements and the other to RIP advertisements. You can extend the standard 60-second IPX periodic SAP advertisement interval for SAP timers by multiples of the update interval that you specify. You configure the interval by specifying the value of the Update Interval parameter, and the multiplier by specifying the Age Multiplier parameter. Refer to Chapter 4 for details on how to configure these parameters. Configuring SAP timers can reduce IPX SAP overhead and enhance bandwidth availability. You can eliminate periodic SAP advertisements by setting configurable SAP timers to zero; thus, only triggered SAP updates will be propagated.

To ensure proper SAP operation, set configurable SAP timers at equal advertisement intervals on all Bay Networks router interfaces attached to common IPX network segments. To alleviate the unnecessary purging of SAP entries, the configurable SAP timers feature also automatically extends an entry's SAP age-out time to three times the value of the SAP advertisement setting of the interface on which the entry was learned. Standard SAP operation purges any SAP table entry for which information is not received (in a SAP update) after 180 seconds (three times the standard 60-second IPX periodic SAP advertisement interval).

Note: *While you can set configurable SAP timers on any Bay Networks router interface, do not use them on LAN interfaces, because IPX servers do not currently support configurable SAP broadcast timers. As a result, IPX servers will purge SAP entries after 180 seconds if they have not received any updates within this time interval.*

Configuring SAP Filters

A filter is a pattern of bits that you specify as a hexadecimal number; for example, 0x0000FFFF. The router scans incoming and outgoing SAP packets to see whether certain fields in the packet match the filter. The type of filter — network-level or server-level — determines which fields the router examines. When you set up the filter, you can specify what the router does with the packet when it finds a match.

You can create SAP filters on Bay Networks routers in your network to regulate both incoming and outgoing SAP advertisements. You can use SAP filters to control the size of resident SAP services tables and reduce bandwidth waste on you network due to SAP broadcast overhead. You can also use SAP filters as a security mechanism to limit a user's view of services located elsewhere on the network.

Each SAP filter consists of a server name or network number, a service type, and a configurable action parameter. As a result, you can tailor SAP filters to your site requirements, improving network security by controlling access and preserving bandwidth by limiting the SAP packet traffic. On a given interface, you can configure a filter as inbound, outbound, or both.

- *Inbound* filters affect only incoming SAP advertisements. The filter determines whether the Bay Networks router accepts or suppresses the service information from certain servers, based upon the action that you specify.
- *Outbound* filters affect only outgoing SAP advertisements. The router either advertises or suppresses SAP information, depending on whether it matches the filter's content, based upon the action that you specify.
- *Both* applies the same filter pattern to both incoming and outgoing SAP advertisements.

Figure 1-11 shows an example of SAP outbound filtering.

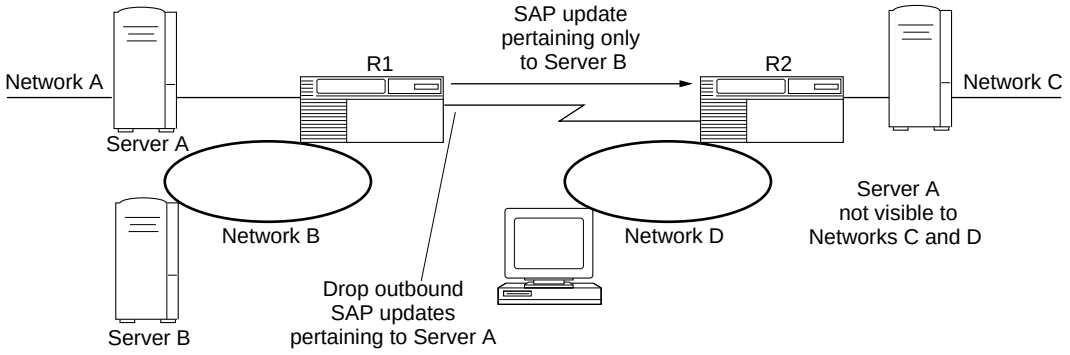

Figure 1-11. SAP Filtering

In this example, a SAP filter configured on Router R1 prevents SAP advertisements and updates pertaining to Server A from being propagated over the wide-area link. As a result, Server A is invisible to Networks C and D. Information pertaining to Server B, however, continues to be propagated over the WAN link.

Note: *While SAP filters restrict a user's view of network service information, they do not prevent users from accessing services. If users have access to resources contained on an IPX network, they can also access all services within that network, regardless of whether a service has been filtered. It's like telling the Post Office to discard all sale flyers that you receive from a certain store. You assume that the store still exists, and you can still go to and buy from that store, even though you may not know its latest specials. The IPX router always updates its own SAP services table according to inbound SAP data.*

You can configure SAP filters using the following levels:

- You can filter SAP service information pertaining to individual servers by editing server-level SAP filters.

  At the service level, the filter matches a pattern that you specify (consisting of a service name pattern and a service type). The filter's Action parameter determines the action (Accept/Advertise or Suppress).

- You can filter service information pertaining to entire networks by editing network-level SAP filters.

  At the network level, the filter matches a pattern that you specify (consisting of a service network number and a service type). The filter's Action parameter determines the action (Accept/Advertise or Suppress).

The IPX router with an outbound filter configured on an interface includes information about a service in a SAP packet if either of the following is true:

- The router finds a match between an outbound filter's contents and the service in its SAP services table, and the filter action is Advertise/Accept.
- The router does not find an outbound filter that matches the service in its SAP services table.

The IPX router excludes information about a service from a SAP packet only if it finds a match between an inbound filter's contents and the contents of its SAP services table, and the filter action is Suppress.

Similarly, the IPX router accepts information about a service in a SAP packet if either of the following is true:

- The router finds a match between an inbound filter's contents and the service in the SAP packet, and the filter action is Advertise/Accept.
- The router does not find an inbound filter that matches the service in the SAP packet.

Static Services

When you statically configure NetWare services, the router learns about a NetWare service by means of the SAP information you enter using Site Manager. You can manually configure NetWare static services for each interface on a Bay Networks router.

When you configure static services on an interface, you can then use SAP filters to eliminate the SAP announcements. This reduces traffic and bandwidth use on the WAN, potentially enhancing WAN performance. Alternatively, you can disable SAP entirely on an individual-interface basis or disable just the SAP immediate update messages. Refer to "Editing SAP Circuit Parameter Descriptions" in Chapter 4 for more information on enabling and disabling SAP broadcasts.

For network topologies that include slower-speed WAN links, reducing the amount of WAN bandwidth otherwise needed for SAP announcements can be

helpful. You can also reduce traffic by setting the Update Interval parameter to zero, which indicates no periodic SAP updates and no aging of SAP information resulting from periodic updates. In this case, SAP immediate updates still propagate through the network. You can also configure the interface to disable immediate updates by setting the Immediate Update parameter.

A service sends an immediate update when one of the following conditions occurs:

- A service first comes up
- A service changes
- A service is no longer available

For more information about the Update Interval parameter, see “Configuring RIP and SAP Broadcast Timers” in this chapter. For instructions on setting the Update Interval and Immediate Update parameters, refer to Chapter 4.

Figure 1-12 shows a sample network configured to use static SAP services. If you want Client 1 to have access only to File Server 3, you configure File Server 3 in the static SAP table on Router 2’s interface. Then, to suppress any SAP broadcasts from Router 1 and thus reduce bandwidth use, you can either turn off the SAP supply or simply disable SAP.

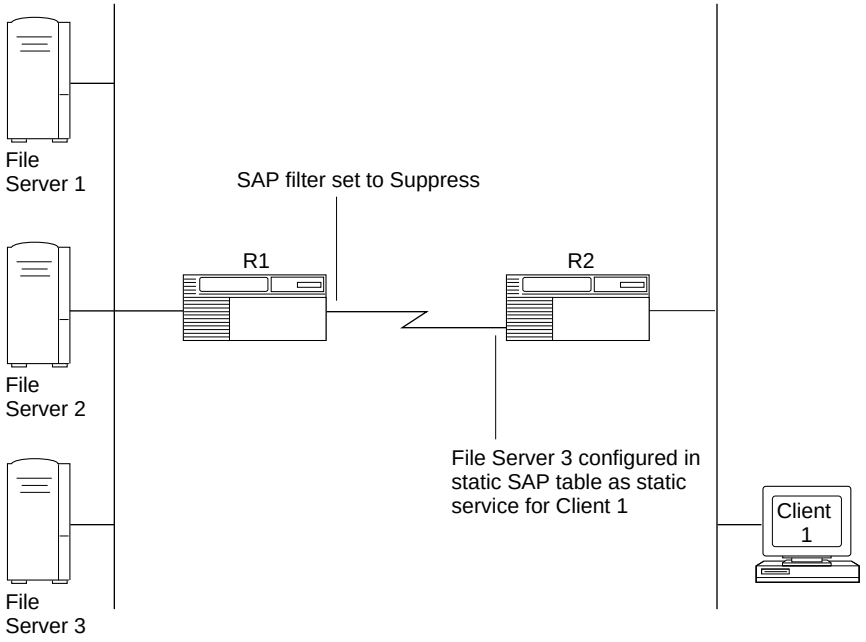

Figure 1-12. Static SAP Service Network Configuration

Figure 1-13 shows another example, in which a SAP filter is configured on Router R1, prohibiting periodic SAP advertisements and triggered SAP updates from being propagated over the wide-area link. As a result, the services resident on Server A or Server B are not visible to Networks C and D. However, SAP services resident on Servers A and B are manually entered into Router R2's SAP table. This way, these servers are visible to IPX endstations on Networks C and D (through periodic SAP advertisements, which are broadcast over Router R2's LAN interfaces every 60 seconds, in conformance with IPX specifications). The key benefit in this example is that SAP overhead is eliminated over the WAN link.

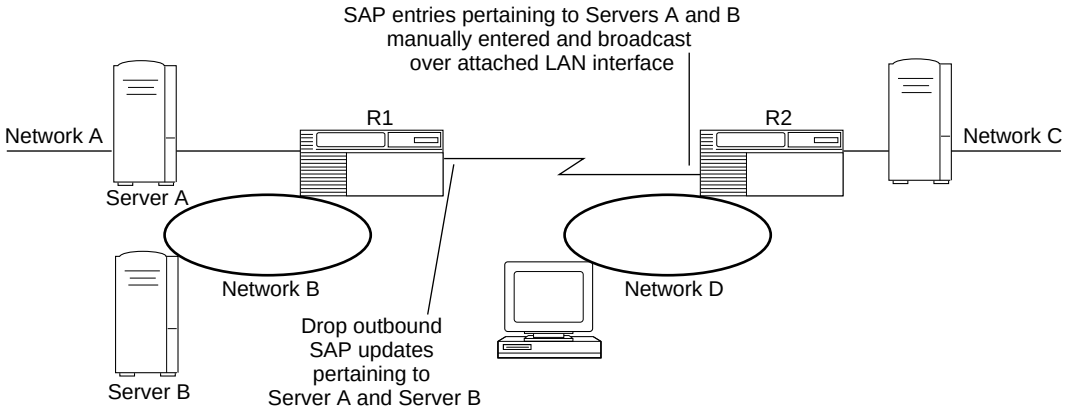

Figure 1-13. IPX SAP Filters Prohibiting SAP Broadcasts

You add, edit, or delete static services through the IPX Static Services window. For instructions, see "Editing Static Service Parameters" in Chapter 4. You can configure only services that have valid network addresses. Valid network addresses are provided either by RIP or by statically configured routes. If you try to enter any services that have invalid network addresses in the router configuration, the router accepts the information, but the services are unreachable.

Note: *Broadcast mechanisms, such as periodic RIP and SAP advertisements, can force dial-on-demand connections to be continuously established, preventing user-defined dial-on-demand expiration time limits from being reached. See the next section for more information.*

Dial-on-Demand

Dial-on-demand is a dial service that offers access to a switched network by means of a dial-up line connection. Dial-up lines are dynamic connections that are active only on an as-needed basis — that is, when there is data to be sent across the network. These lines can be a cost-effective alternative to leased lines and packet networks, which are available all the time, regardless of network traffic.

For users who send a limited amount of data or whose data transmission is not constant, dial-up lines can be less expensive than leased lines, and they can maximize network performance and flexibility.

Dial-on-demand and dial backup services work over any public switched network, such as the standard telephone network, a switched 56 Kb/s network, and an Integrated Services Digital Network (ISDN).

This section provides a brief overview of dial-on-demand service. Refer to *Configuring Dial Services* for a detailed description of this service.

Using Dial-on-Demand Service

Dial-on-demand lets you establish a circuit only when you need it, as opposed to having a leased-line connection. With dial-on-demand, you establish a network connection only when the router has data to send across the network or when you have manually configured the router to establish a connection; for example, at a preset time. Dial-on-demand supports synchronous lines (RS232, V.35, RS422, and X.21) and ISDN interfaces.

When dial-on-demand is configured, the router activates a dial-on-demand circuit for any one of the following reasons:

- **The router has data to send across the circuit.**

  When the router has data to transmit, it automatically selects one of the demand lines from the circuit's associated demand pool. As long as data is going across the line, the end-to-end connection remains active.

- **You have specified a time of day to activate the circuit.**

  When you specified a time of day to activate the circuit by configuring a parameter to bring up the circuit (Bring Up Hour/Bring Up Minute) and a parameter to take down the circuit (Take Down Hour/Take Down Minute).

  Using these parameters, you can instruct the router to activate/deactivate a connection during a specific time interval. With these parameters set, the router ignores the Inactivity Time parameter that it uses to dynamically bring down the connection.

- **You enabled a force dial. The router forces the establishment of a circuit.**

  You enabled the Force Dial parameter to immediately activate a line and establish a connection. Using this parameter, you can force the connection to come up, regardless of whether there is data activity.

The router brings down the circuit for any one of these reasons:

- **The configured inactivity time expires.**
- **You scheduled the circuit to come down.**
- **You enabled a force take down.**

Figure 1-14 shows a dial-on-demand line connecting two routers. In this example, when the router has data to transmit across a demand circuit, or when you configure the router to bring up a demand circuit, the router instructs the dial device to establish a connection.

Note: *Don't configure IPX adjacent hosts with dial-on-demand circuits.*

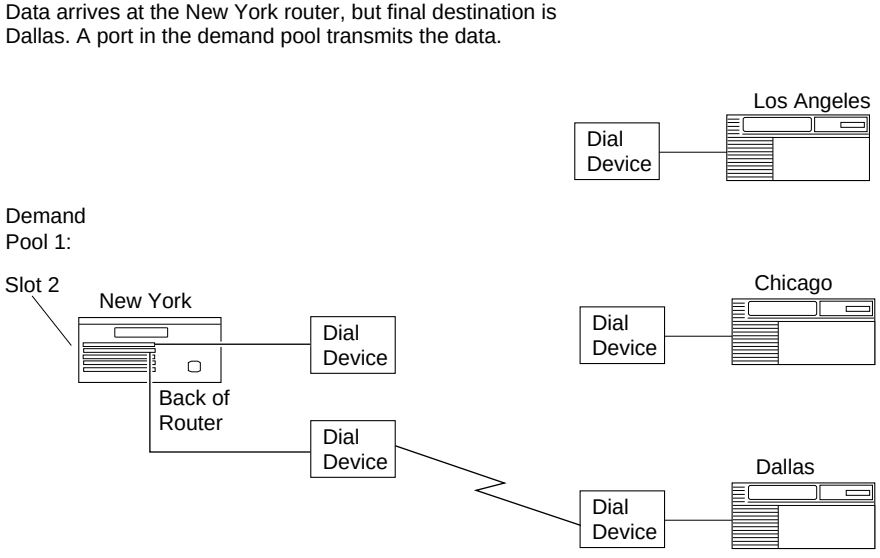

Figure 1-14. Dial-on-Demand Service

Using Static Routing with Dial-on-Demand

As part of its standard operation, IPX sends update packets to maintain routing tables and to gather information about network resources. For dial-on-demand, the frequency of these update packets forces the dial-up connection to remain up permanently, unless you configure a time of day to bring the connection down.

When you configure dial-on-demand circuits, you should disable broadcast messages. The router then uses static routes to determine the location of the destination network.

Tips for Using Dial-on-Demand with IPX

The following suggestions may help improve overall system efficiency if you're using dial-on-demand with IPX:

- Turn off triggered updates.
- Set the periodic update interval to a large value — the line will be called only infrequently.
- Use service filtering and/or route filtering.
- Use static routes and static services.
- Use the default route.
- Enable local watchdog acknowledgment ("spoofing").
- Use traffic filters and protocol prioritization to prohibit routing updates and protocol-specific messages from keeping the circuit up unnecessarily (see *Configuring Traffic Filters and Protocol Prioritization* for details).

Local IPX Watchdog Acknowledgment

In a NetWare network, NetWare servers broadcast "watchdog" packets every 2 minutes to verify that client nodes are still connected to the server. Watchdog packets are just another form of data packet.

To maintain the connection, the client must respond to this watchdog message (essentially, responding to a poll). With a dial-up connection (that is, when you want to establish periodic connectivity to a remote site using the dial-on-demand feature), this polling mechanism could mean dialing the phone line just to keep the server from bringing down the connection.

In addition, the bandwidth consumed by periodic RIP/SAP and watchdog broadcast packets can represent a significant portion of the total dial cost when charged on a per-packet basis. Depending on the network configuration and the application, this excessive broadcast activity can reduce application access performance.

To address this problem, Bay Networks routers can use local watchdog acknowledgment to improve the efficiency of IPX wide-area links. This feature, also known as "watchdog spoofing," lets Bay networks routers locally respond to broadcast IPX watchdog packets on behalf or clients connected over dial-in connections.

Without local watchdog acknowledgment, each time a server sends an IPX watchdog packet to a logically connected client, the dial-on-demand link will be established and remain up to support the communication between the client and the server (that is, the watchdog packets).

Within an IPX network, servers rely on client watchdog acknowledgments to verify that client sessions are still active with the server. The router closest to the server responds on behalf of the client. As a result, NetWare servers may reach the maximum client sessions supported by the server, although not all clients are truly maintaining a session. This can happen if the client does not perform a standard closure of the session; for example, if the client PC is rebooted. You can avoid this potential problem by implementing NetWare's auto logoff feature to ensure that client sessions are released when they are no longer in use.

NetBIOS Static Routing

NetBIOS establishes sessions (logical connections) and allows for communication between PCs. The Bay Networks NetBIOS static route function lets you map NetBIOS names to IPX destination networks by configuring a NetBIOS static route to a NetBIOS service name. The IPX router then converts the broadcast NetBIOS packets to directed broadcast NetBIOS packets, which are usually forwarded to all network interfaces on a single network. This reduces the amount of network traffic due to NetBIOS query requests; that is, broadcasts issued by NetBIOS clients seeking to find and establish sessions with specific NetBIOS applications over an IPX internetwork.

Besides minimizing NetBIOS broadcast traffic, using NetBIOS static routes allows a more precise logical partitioning of an IPX NetBIOS internetwork, enhancing internetwork security.

The Bay Networks IPX router software lets you specify whether:

- You want to direct a NetBIOS broadcast (Type 20) packet through a network by configuring a static route only at the first router. Before the packet is directed out an interface, the router software overwrites the IPX destination address of the packet so that it can be routed to its destination. Because the IPX specification states that the network address of broadcast packets must be left unchanged, this option does not conform to Novell standards.
- You want the router to propagate a packet out all of its interfaces (in conformance with Novell standards).
- You want to direct a packet to its destination by configuring a static route for each hop in the network (in conformance with Novell standards).

In the NetWare environment, NetBIOS query requests are encapsulated within IPX packets. When a Bay Networks router receives an IPX packet containing a NetBIOS query request, it compares the NetBIOS name for which a connection is being requested to a statically configured NetBIOS Name-to-IPX Destination Network table. If the requested NetBIOS name matches a table entry, the Bay Networks router forwards the query request packet out only one IPX interface toward the destination network. If a match does not exist, the router propagates the query request packet out of all IPX interfaces, in conformance with the IPX specification. For details on configuring standard NetBIOS operation over IPX, refer to Chapter 4.

In Figure 1-15, for example, when End System ES2 wants to find and establish a connection to a NetBIOS application on the IPX Server ES2, it generates a query request broadcast packet. Router R1 receives the broadcast packet, consults its NetBIOS Name-to-IPX Destination Network table, finds that the NetBIOS application being requested is mapped to Network B, and routes the packet out Interface 1. Similarly, Router R3 consults its NetBIOS Name-to-IPX Destination Network table upon receiving the NetBIOS query request, and routes the packet out its interface to Network B.

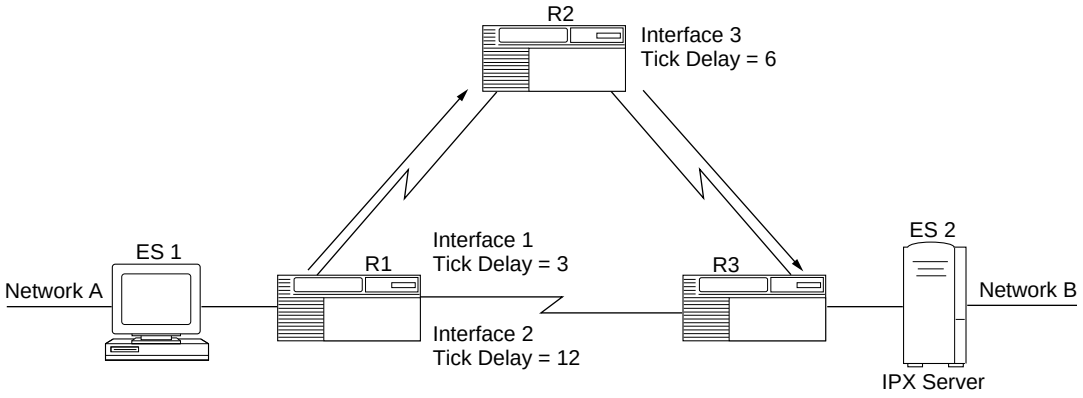

Figure 1-15. NetBIOS Static Routes

You set up NetBIOS static routes through the Configuration Manager. Then, from the Configuration Manager Protocols menu, select IPX (not IP). From the cascaded menu select the NetBIOS Static Routes option and fill in the fields in the subsequent windows.

Each IPX router interface supports up to 50 NetBIOS static routes. Each NetBIOS static route specifies a NetBIOS resource name and a destination network where the resource resides.

Directing a NetBIOS Packet Using Nonstandard Static Routing

You can direct a NetBIOS packet through a network by configuring a NetBIOS static route in the first Bay Networks router to receive a NetBIOS broadcast packet. To do this, you must set the Novell Certification Conformance parameter on the Edit IPX Advanced Global Parameters window to Disabled for all routers in the network. All NetBIOS packets sent from a client to the router must have a destination network value of zero, unless the packet passes a static route in the router. The router tests a packet against the static route table before it checks the packet's destination, thus allowing the router to accept packets that may not have a destination network of zero.

Caution: *This method of defining IPX NetBIOS static routes is a nonstandard Bay Networks feature that may not be compatible with routers from other vendors.*

This method converts a NetBIOS broadcast packet to a NetBIOS directed broadcast packet, thereby eliminating the loop checking and path tracing that is usually done for NetBIOS broadcast packets. This may cause problems with applications that rely on those mechanisms.

When you configure a NetBIOS static route, the IPX router inserts the network number configured in the static route into the destination network number of the IPX packet. Refer to Chapter 4 for instructions on how to add a NetBIOS static route to an IPX interface.

When you configure NetBIOS static routes on an interface, the IPX router compares all IPX NetBIOS broadcast packets received on the interface with the boxwide NetBIOS static routes. If the NetBIOS destination name found in the packet matches an entry in the routing table, the NetBIOS packet is routed to the associated destination network. If no match is found, the IPX router treats the packet as specified by the NetBIOS Accept and NetBIOS Deliver parameters. Refer to the descriptions of the NetBIOS Accept and Deliver parameters in Chapter 4 for more information.

Forwarding Packets Out All Interfaces

To configure a router to propagate a packet out all of its interfaces — which conforms to Novell standards — you set the Novell Certification Conformance parameter on the Edit IPX Advanced Global Parameters window to Enable. You must set this parameter to Enable for all routers on the network.

To control the flow of NetBIOS traffic, you can use the NetBIOS Accept and Deliver parameters to determine whether you want an interface to accept NetBIOS broadcast broadcasts from an attached network and to deliver NetBIOS broadcasts to a network. Refer to the descriptions of the NetBIOS Accept and Deliver parameters in Chapter 4.

Directing a NetBIOS Packet Using Standard Static Routing

If you want to configure NetBIOS static routes in conformance to Novell standards, you must configure a static route for each hop in the network. You configure a NetBIOS static route to a NetBIOS name on the IPX Interfaces window (Figure 1-16).

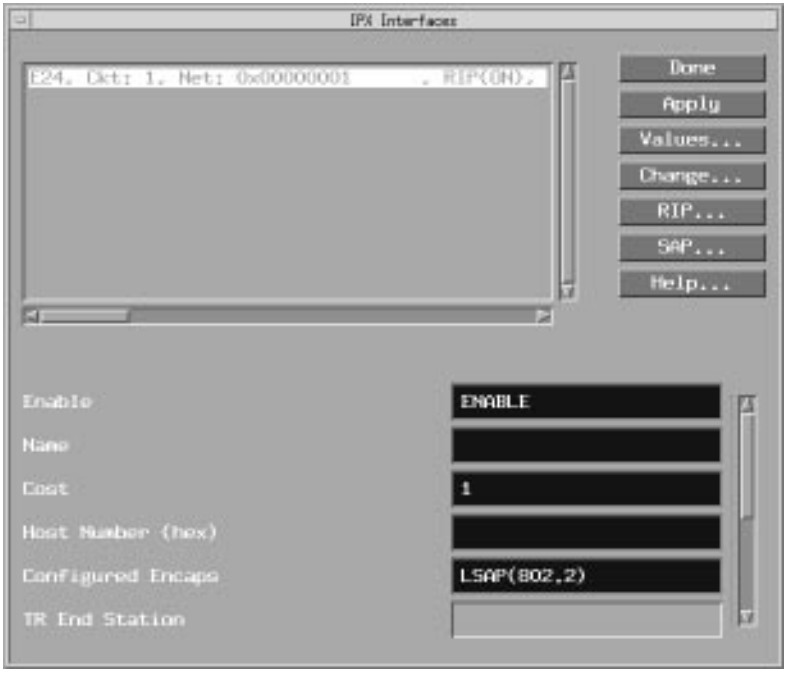

Figure 1-16. IPX Interfaces Window

Scroll down until you see the parameter field. After you specify the static route to a NetBIOS name, the IPX router converts standard NetBIOS broadcast packets to NetBIOS *directed* broadcast packets.

- NetBIOS broadcast packets are sent to all accessible host IDs on *all* accessible IPX networks.
- NetBIOS directed broadcast packets are sent to all host IDs on a *single* IPX network.

Chapter 4 describes in detail how to add a NetBIOS static route to an IPX interface.

NetBIOS Broadcast Filters

You can control the propagation of IPX NetBIOS broadcasts by configuring NetBIOS broadcast filters on an interface. This feature ensures that visibility to NetBIOS resources is limited only to networks that need to have access to certain resources. You can configure an interface to either accept or not accept NetBIOS broadcasts from an attached network, and to deliver or not deliver NetBIOS broadcasts to a network. This capability can enhance security and preserve bandwidth by controlling the flow of NetBIOS traffic.

The NetBIOS Accept and NetBIOS Deliver parameters on the IPX Interfaces window let you configure each interface to accept and forward NetBIOS broadcasts. By default, both of these parameters are enabled.

Note: *The description that follows assumes that the NetBIOS destination name found in the packet does not match an entry in the NetBIOS Static Routing table.*

With NetBIOS Accept enabled on an interface, the IPX router accepts NetBIOS broadcast packets received on that interface. For example, in Figure 1-17, the IPX router accepts NetBIOS broadcast packets received only on Interfaces 1 and 2, because the Accept parameter for those interfaces is set to Enabled.

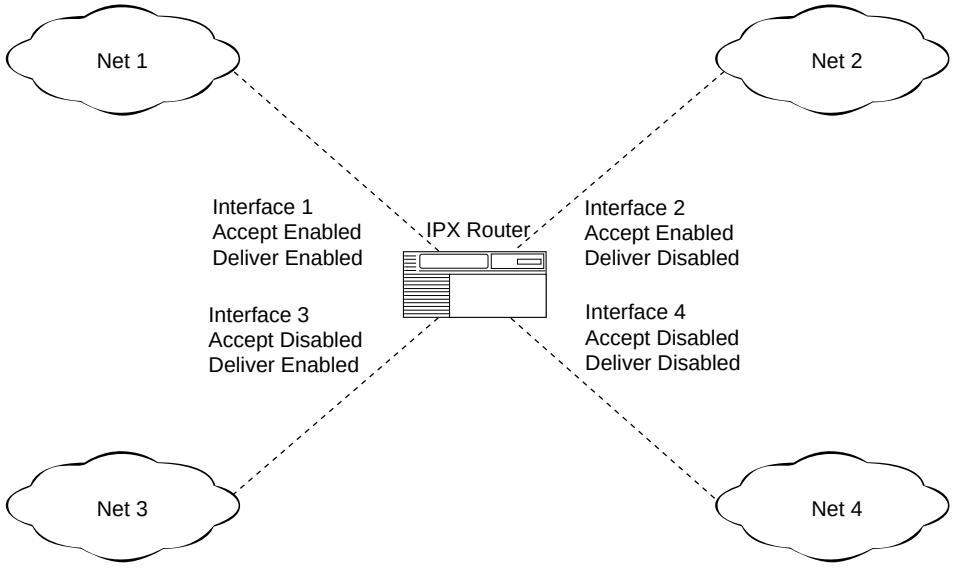

Figure 1-17. NetBIOS Packet Filtering

With Deliver enabled on an interface, the IPX router delivers NetBIOS broadcast packets that are routed to that interface. For example, in Figure 1-17, the IPX router delivers NetBIOS broadcast packets only to Interfaces 1 and 3, because the Deliver parameter for those interfaces is set to Enabled (and it's set to Disabled for the other interfaces). The arrows in Figure 1-18 show the flow of packets in this same model.

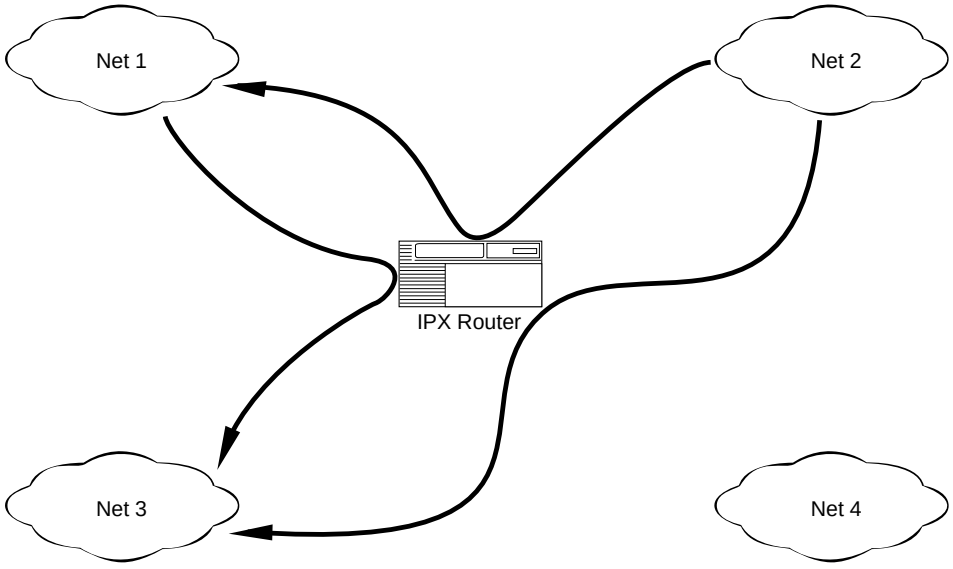

Figure 1-18. NetBIOS Packet Flow

The Accept parameter of the interface receiving NetBIOS broadcast packets and the Deliver parameter of the other interface must both be set to Enabled for delivery of such packets to occur. For example, Interface 1 can deliver only packets from Interface 2 to Net 1, because Interface 2 is the only other interface whose Accept parameter is set to Enabled.

Thus, NetBIOS client applications on Network 1 can initiate and establish sessions with NetBIOS server applications only on Network 3. NetBIOS client applications on Network 2 can initiate and establish sessions with NetBIOS server applications only on Networks 1 and 3. Client applications on Networks 3 and 4 cannot initiate any sessions with NetBIOS server applications via the IPX router.

As another example, in Figure 1-19, NetBIOS broadcasts from the End System ES1 on Network A are *accepted* by Router R1, but can be prohibited from Network C by setting the Deliver parameter on the interface of Router R1 connected to Network C to Disable. NetBIOS broadcasts will still be delivered on Network B.

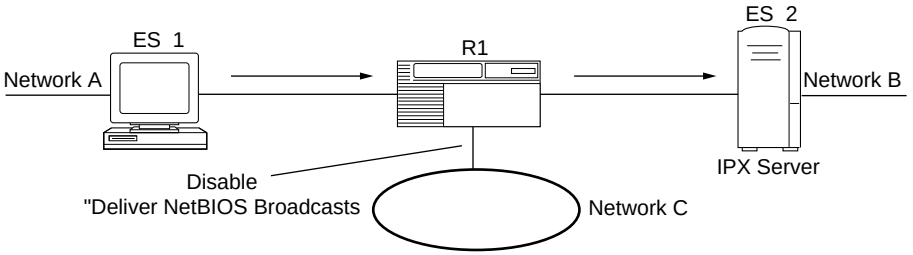

Figure 1-19. NetBIOS Broadcast Filtering

Refer to “Editing IPX Interface Parameters” in Chapter 4 for instructions on how to disable the NetBIOS Accept and Deliver parameters.

Source Route Bridge Endstation Support

Source route bridge endstation support enables routable traffic generated in a source route bridge environment to be routed to workstations on remote LANs over a multiprotocol backbone. The Bay Networks router running IPX lets you configure source route endstation support for Token Ring networks on each interface. This allows bridging and routing to coexist in the same IBM source route bridging environment. With endstation support enabled, endstations that support both source route bridging and IPX can use source routing to traverse bridged networks.

In a source routing network, every endstation supplies each frame it sends out with route descriptors, so that it can be source routed across the network. Thus, in order for routers running IPX to route packets across a source routing network, they must act like endstations, supplying route descriptors within each packet before sending it onto the network.

All traffic is source route bridged within the local Token Ring environment. Routable traffic intended for a destination on a LAN interconnected through a multiprotocol backbone is routed over the backbone by the Bay Networks node. With endstation support enabled, the Bay networks router running IPX does the following whenever it receives a packet and determines that the packet’s next hop is across a source routing network:

- Sends out a Single Route Explorer (SRE) frame to discover a path to the next-hop network.
- Adds the necessary Routing Information Field (RIF) information to the packet's MAC header.
- Sends the packet to the network, where it is source routed toward the next hop.

After the peer router receives the packet from the Token Ring network, it strips off the RIF field and continues to route the packet toward the destination network address, as shown in Figure 1-20.

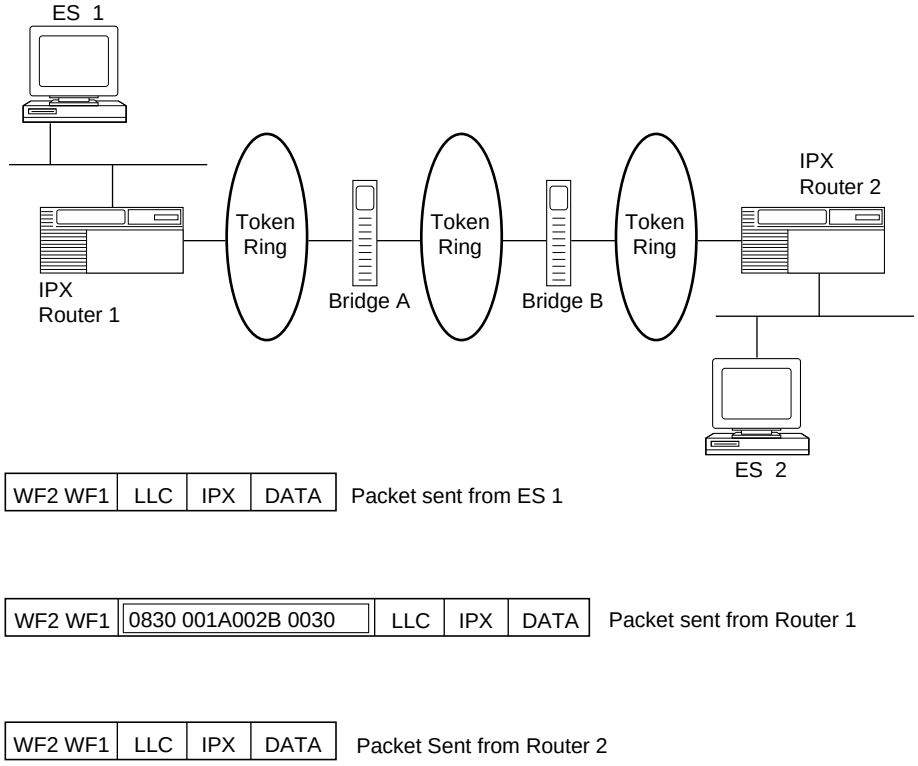

Figure 1-20. IPX Routers Source Routing across a Token Ring Network

You configure source route endstation support on each interface by setting the TR End Station parameter to Enable. See the section "Editing IPX Interface Parameters" in Chapter 4 for instructions on configuring this parameter.

The transition to network-layer routing outside the source route bridge environment can improve overall network performance by reducing source route bridge overhead on a WAN and can maximize network availability by rapidly rerouting around a failed link.

IPX Ping Support

The Bay Networks Site Manager supports the IPX ping feature, which uses an IPX diagnostic packet to ping NetWare servers to determine the accessibility — that is, the status, "alive" or "not responding" — of the following:

- A remote Bay Networks router
- A Novell IPX server (except as noted below)
- A Novell multiprotocol router
- A NetWare client

This feature can be particularly useful in troubleshooting large networks.

Note: *In conformance with the Novell specification, a Bay Networks router running IPX will respond to pings from NetWare servers but will not initiate pings to those servers. Instead, the router running IPX will use diagnostic packets to accomplish the ping function.*

Using the IPX ping command, the router attempts to communicate with another router running IPX, a server, or an IPX client, and determines whether the destination node is functioning and reachable from the source node. The "pinging" Bay Networks router sends an IPX diagnostic packet, called a *Configuration Request*, and either the "pinged" router running IPX, the server, or the IPX client responds with a *Configure Response* packet. See *Managing Routers and BNX Platforms* for instructions on using the ping feature in IPX.

Role of Bay Networks Routers in a Client/Server Connection

This section describes how Bay Networks routers running IPX provide clients access to servers on an IPX internetwork.

- **Router builds SAP and RIP tables**

  The Bay networks router builds its routing and services tables by listening to regularly scheduled SAP and RIP broadcasts from file servers. The broadcasts include the services a server has to offer and routes to a server. If regular SAP or RIP broadcasts from a file server stops, the local router ages out the entry and removes it from its services or route table.

- **Client sends *get_nearest_service/get_nearest_directory_server* SAP request**

  A client sends this request to locate a file server. (Refer to the book, *Novell's Guide to NetWare LAN Analysis*, by Laura Chappell and Dan E. Hawkes, for more information on this mechanism.)

- **Router decisions**

  If the server resides on the same network as the client, the server receives the request and responds. The local router does not respond because its services table indicates that the service is available on the client's network. In this case, client-router communications stop until the client sends the next *get_nearest_service* SAP request.

  If the server does not reside on the same network, the router responds, because its services table indicates that the service is not available on the client's network. The SAP response sent by the router contains the server name, the internal address (if applicable), the service type, the socket number, and the intervening network count of the nearest device offering the service. Continue to the next bullet.

  If the server does not reside on the same network and multiple servers of the same service type are available, the router picks the server that is the fewest ticks away. If two servers are the same number of ticks away, then the router chooses the server that is the lowest number of hops away. If two servers are the same number of ticks and hops away, then the router chooses based on the alphanumeric order of the server names listed in the services table.

- **Client's RIP request**

  The client then broadcasts a RIP request packet to the local segment. This packet requests the best path to the server's network.

- **Router's RIP response**

  The router on the same network as the client refers to its route table and sends a RIP response to the client. The RIP response identifies the network on which the client resides. The RIP response also contains the server's internal network address and the intervening hop and tick count.

- **Client's NCP Request**

  The client sends a Network Core Protocol (NCP) create connection request to the server. The request includes the router's MAC address as the destination address at the data link layer. Within the IPX header, the destination network address is the internal address and the destination node address of the file server. The client forwards the packet to the router.

- **Router forwards packet**

  The router running IPX forwards the packet to the network identified by the destination network address.

Example of Client/Server Connection via Bay Networks Router

In the example shown in Figure 1-21, Client A sends a SAP request to locate a file server. Here's what happens as a result of that request.

1. Because the server does not reside on LAN A (the same LAN as Client A), the Bay Networks IPX router, Host 2, sends a SAP response to Client A, informing it that the File Server, Host 3 on Token-Ring 6, is the nearest device offering the requested service.
2. Client A then sends a RIP request to determine the best path to Host 3.
3. The Bay Networks IPX router, Host 2, sends a RIP response to Client A that includes the server's internal network address and the intervening hop and tick count from Host 3 to Client A.
4. Client A sends an NCP request packet to the Bay Networks IPX router, Host 2.
5. The router then forwards the packet to Host 3.

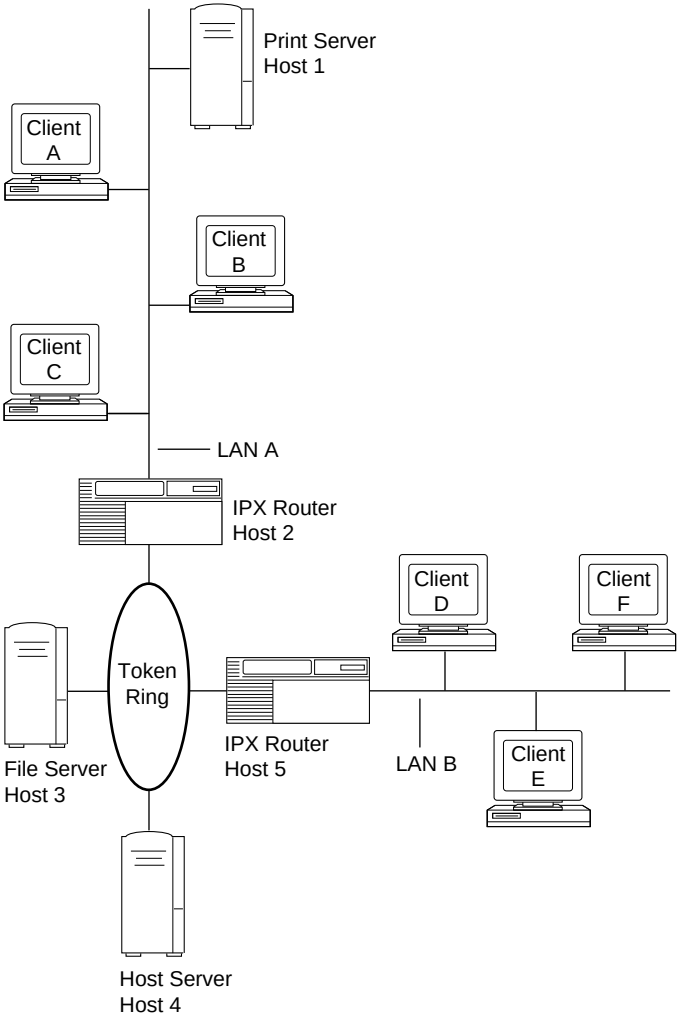

Figure 1-21. Sample IPX Network

For More Information about IPX

The following documents provide technical detail on IPX protocol implementation.

RFC 1634: *Novell IPX over Various WAN Media (IPXWAN)*. (Obsoletes RFC 1551 and RFC 1362.)

RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP)*.

Novell, Inc. *Advanced NetWare, V.2.0 Internet Packet Exchange Protocol (IPX) with Asynchronous Event Scheduler*. March 19, 1986.

Novell, Inc., *IPX Router Specification*. October 1993.

Novell Press/Sybex, *Novell's Guide to NetWare LAN Analysis*, Laura Chappell and Dan E. Hawkes. 1994.

Chapter 2
IPX Configuration and Parameter Requirements

The basic types of IPX configurations are

- Standard, with two possible configurations:
  - — *Multiple-Host Router.* This common configuration supports one IPX interface per circuit; each interface has a unique IPX host number.
  - — *Single-Host Router.* This configuration supports one IPX interface per circuit; every interface shares the same global (“boxwide”) IPX host number.
- Special, also with two possible configurations:
  - — *Multiple Interfaces per Circuit.* This special configuration supports as many IPX interfaces per circuit as there are frame encapsulation types for the given circuit type.
  - — *Multiple Circuits per Segment.* This special configuration supports either concurrent bridging and IPX routing or IPX multiline.

Standard IPX Configurations

You can configure your Bay Networks router to serve as either a multiple-host or single-host router.

Multiple-Host Router

For this configuration, leave the Multiple Host Address Enable parameter at its default setting, Enable. The host number of each IPX interface is based on the MAC address of the underlying circuit. For more information about the Multiple Host Address Enable parameter, see Chapter 4 of this manual. The only decision

you need to make is whether the source of the MAC address is a PROM on the circuit or a MAC Address Override entry that you specify for the circuit.

You specify the source for the MAC address by means of the MAC Address Select parameter. For more information about the MAC Address Override and MAC Address Select Token Ring line detail parameters, see *Configuring Line Services*. For more information about setting the MAC Address Select parameter for IPX, refer to "Token Ring MAC Address Selection" later in this chapter.

Single-Host Router

For this configuration, you need to set the Multiple Host Address parameter to Disabled. Every IPX interface in the router configuration uses the same global host number, which is one of the following:

- A number derived from the router backplane
- A number that you enter into the Router Host Number parameter field

You specify the source for the host number by entering a host number in the Host Number field of the IPX Global Parameters window. (If you do not enter a number, the router derives the internal serial number from the router backplane, and uses this number for the global host number.) For more information on how to access and edit IPX global parameters, refer to Chapter 4.

Special IPX Configurations

You can also configure your router to support multiple interfaces per circuit or multiple circuits per segment.

Multiple Interfaces per Circuit

IPX configurations with multiple interfaces per router circuit typically support migration from an existing release of Novell IPX to a later release. For this type of configuration, you must set the following parameters according to the guidelines that follow:

- Multiple-Host Address Enable
- Host Number
- MAC Address Select

- MAC Address Override
- Network Number
- Configured Encapsulation Type

Multiple-Host Addressing, Host Numbers, and MAC Addresses

If you have multiple IPX interfaces per circuit, leave the Multiple Host Address Enable parameter at its default setting of Enabled. The source for the host number of each IPX interface depends on the circuit type.

If the circuit type is Token Ring, each IPX interface adopts as its host number the MAC address value established for the circuit. The only choice you need to make is whether the source of the MAC address that an interface uses for a host number is

- A PROM on the circuit
- A MAC Address Override value that you enter for the circuit
- The global internal serial number derived automatically from the router backplane

You select a source for the MAC address by means of the MAC Address Select parameter on the Token Ring Configuration window. For more information on this parameter, refer to “Token Ring MAC Address Selection” later in this chapter.

If the circuit type is Ethernet or any other circuit type that supports selective operation, then you select a source for the host number by entering a host number in the Host Number field of the IPX Interface Parameters window. (If you do not enter a number, the router uses the value you specified for the MAC address.) For more information on how to access and edit IPX interface parameters, refer to Chapter 4.

Network Numbers

When you initially add an IPX interface to the router configuration, the Configuration Manager tool requires you to enter the network number of the IPX network segment associated with that interface. The network number has a nonzero value for all IPX interfaces except

- Interfaces with IPXWAN
- Interfaces with unnumbered point-to-point links and without IPXWAN enabled

The network number must be unique among all other network numbers assigned throughout the IPX internetwork.

Specify a network number of zero. See *Configuring Routers* for instructions. The router recognizes a network number of zero on an interface as an indication that a lower protocol layer (IPXWAN or IPXCP) on the same circuit must negotiate with the remote IPX host for the network number of the intervening WAN segment. Next, for IPXWAN only, you must enter a primary network number and a unique router name in the Edit IPX Global Parameters window. You can enter zero for the primary network number for point-to-point links without disabling IPXWAN. In addition, you must specify a unique common network number in the IPX Interfaces window for that interface.

Frame Encapsulation Types and the Number of IPX Interfaces per Circuit

When you add an IPX interface to the router configuration, you must set the Configured Encaps parameter according to the type of frame encapsulation required for communication between all clients on the same IPX logical network within the overall IPX internetwork.

You can configure as many logical interfaces on a circuit as there are encapsulation types available for that type of circuit. For example, you can configure four *different* encapsulations for four independent IPX interfaces on a single Ethernet circuit (Ethernet, Novell, LSAP, and SNAP). Each interface and encapsulation configured on a circuit supports a different logical network.

The Bay Networks Site Manager software lets you choose for an IPX interface only those encapsulations that are appropriate for the type of physical circuit, as follows:

- Ethernet circuits support Ethernet, LSAP (802.2), Novell (802.3), and SNAP frames.
- Token Ring circuits support LSAP and SNAP frames.
- FDDI circuits support LSAP and SNAP frames.
- Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support ATM SNAP, Frame Relay SNAP, PPP, SMDS SNAP, and Bay Networks Point-to-Point (Ethernet) frames.
- HSSI circuits support ATM SNAP, Frame Relay SNAP, PPP, SMDS SNAP, and Bay Networks Point-to-Point (Ethernet) frames.
- ISDN circuits support PPP.

Multiple Circuits per Segment

This special configuration supports either

- Concurrent bridging and IPX routing
- IPX multiline

Refer to Chapter 1 for information on IPX multiline configurations. You can configure bridging as described in *Configuring Bridging Services*.

IPX Host ID Numbers

On Bay Networks routers, the IPX host ID number maps to a physical data link layer address (on a specific circuit or physical interface). An IPX logical interface can listen at this address and capture frames transmitted by nodes compatible with IPX on the local data link.

Figure 2-1 illustrates this concept in a Bay Networks router that has two IPX logical interfaces, each one configured on a different physical circuit.

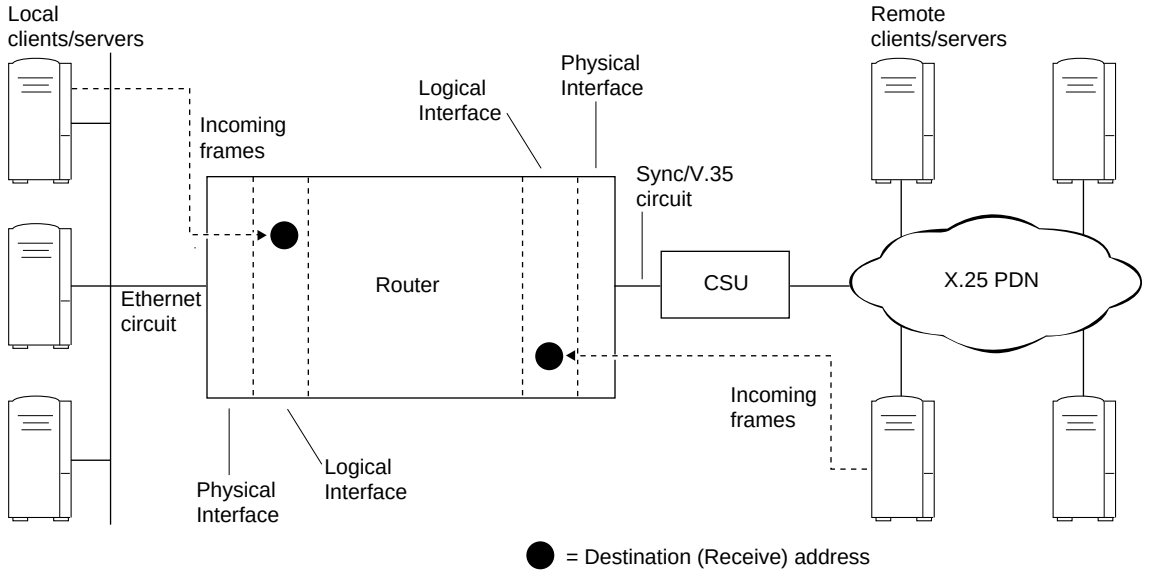

Figure 2-1. Frames Received at a Logical Interface

IPX compatible nodes on the same logical network and locally attached physical segment must use the host ID number of the IPX logical interface as a data link layer destination address, through which any transmitted frames can ultimately reach their target client or server applications.

Because an IPX logical interface can receive and send data, the host ID also identifies a source data link layer address from which the interface can send frames to nodes compatible with IPX anywhere else in the same IPX internetwork.

Figure 2-2 illustrates this concept in a Bay Networks router configured with two IPX logical interfaces, each one on a different physical circuit type.

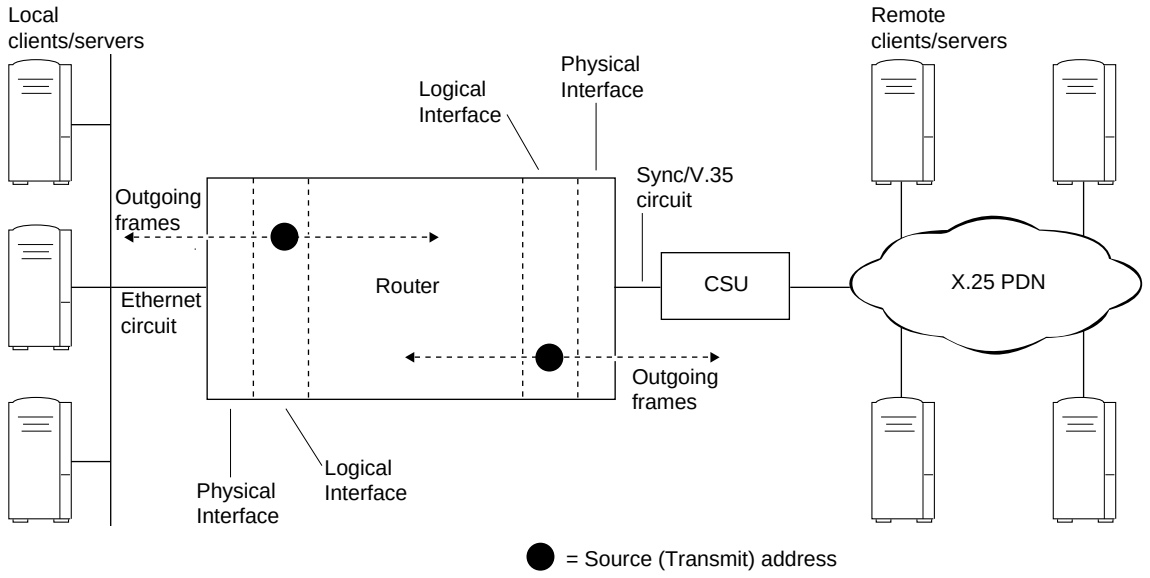

Figure 2-2. Frames Issued from a Logical Interface

Host ID Number for IPX on a Token Ring Circuit

In a configuration with IPX logical interfaces on a Token Ring circuit, the data link layer address is a MAC-layer address.

In Bay Networks routers, you set the MAC-layer address for the circuit and the host ID number for the IPX interface independently. However, the host ID number

for every IPX logical interface on a given Token Ring circuit must be identical to the MAC address set for that circuit. Otherwise, the logical interface would send frames that contained an incorrect source MAC address, or the interface would listen for frames at the wrong MAC address.

Token Ring MAC Address Selection

For Token Ring circuits, you can select the means by which the router determines the MAC address for a circuit by setting the MAC Address Select parameter on the Token Ring configuration window for that circuit to one of the following:

- PROM. (This is the default setting.) The circuit retrieves the MAC address that is stored in a PROM on the supporting link module.
- BOXWIDE. The circuit generates a MAC address based on the serial number of the backplane of the router.
- CNFG. You can configure a MAC address.

Caution: *The IPX boxwide host address and the Token Ring MAC address must agree when the Multiple Host Address parameter is disabled.*

For instructions on how to set the MAC Address Select parameter, see *Configuring Line Services*.

Caution: *Changing the setting of the MAC Address Select parameter to accommodate IPX configuration requirements may have secondary effects on other protocol interfaces (for example, LNM Servers or IP) configured on the same circuit(s) with IPX. If necessary, make adjustments to the parameter settings of any such (non-IPX) interfaces configured on the router.*

If you choose the CNFG option of the MAC Address Select parameter, you must subsequently enter a valid MAC address in the MAC Address Override parameter. You must repeat this procedure on any Token Ring circuit for which you choose CNFG (user configured) as the source for the MAC address assigned to the individual physical circuit.

Host ID Number for IPX over ATM

To establish an IPX connection over an ATM network, you must assign a unique host ID number to the ATM interface that is running IPX. To assign a number, you can either

- Enter a value using the Host Number parameter, which is located on the IPX Interface Parameters window
- Specify that the global MAC address be used for the host ID by disabling the Multiple Host Address Enable parameter, which is located on the Edit IPX Global Parameter window

For instructions on configuring the Host Number and the Multiple Host Address Enable parameters, see Chapter 4.

Configuring IPX without RIP

The IPX router learns WAN network addresses from RIP and SAP broadcasts received over wide area networks. The router stores the IPX host address/WAN address pairs for future determination of next-hop destinations.

To reduce the size of these routing tables and reduce bandwidth, you may want to configure IPX without RIP. However, you must perform the following steps when you configure a WAN IPX interface without RIP:

1. **Configure an adjacent host, and edit the WAN Address parameter in the IPX Adjacent Hosts window for each host on an adjacent Frame Relay, ATM, or SMDS network.**

Note: *The only time you configure adjacent hosts is when you do not have RIP configured on the interface, and you are running IPX over Frame Relay, ATM, or SMDS.*

Refer to the section “Editing an Adjacent Host” in Chapter 4 for detailed instructions.

2. **Configure a static route to the next-hop router for each remote network. The next-hop host will be the adjacent host.**

Refer to the section “Editing a Static Route” in Chapter 4 for detailed instructions.

Chapter 3
Enabling IPX and IPXWAN Services

This chapter describes how to enable IPX and IPXWAN services on a circuit. It assumes that you have read *Configuring Routers* and that you have

1. Opened a configuration file.
2. Specified router hardware, if this is a local mode configuration file.
3. Selected the link or net module connector on which you are enabling IPX services or configured a WAN circuit if this connector requires one (for IPXWAN services).
4. Selected an appropriate WAN protocol from the WAN Protocols window. For an IPXWAN interface, you must select either PPP or Frame Relay. Selecting Frame Relay, PPP, or SMDS on a circuit automatically enables protocol prioritization.
5. Selected either IPX or RIP/SAP from the Select Protocols window.

When you enable these services, you are required to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters.

Enabling IPX and IPXWAN on a Circuit

You enable IPX and IPXWAN services from the IPX Configuration window (Figure 3-2), which appears when you click on OK in the Select Protocols window. Refer to the parameter descriptions in this section to specify the parameters.

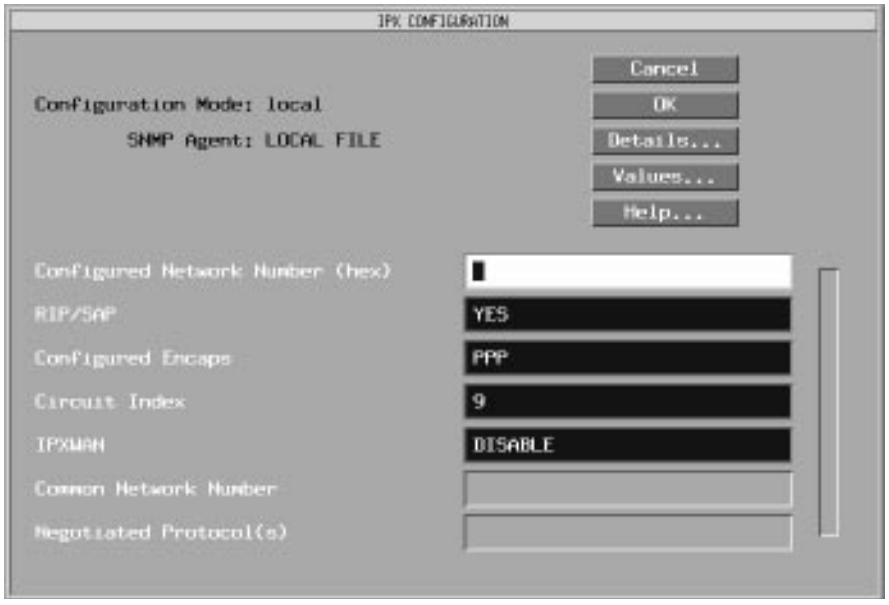

Figure 3-1. IPX Configuration Window

Note: *The Negotiated Protocols field is available only for circuits for which you enable IPXWAN. For IPXWAN services, you can enter values into the Negotiated Protocols field as hexadecimal numbers or you can click on Values for a popup menu selection. Your selection appears on the IPX Configuration window as a hexadecimal number.*

Configure the parameters on this window according to the parameter descriptions that follow. When you have specified all parameters in the window, you can either click on OK to enable default IPX services and to display the next protocol-specific pop-up window, or click on Details to edit the default values.

IPX and IPXWAN Parameter Descriptions

Use the following descriptions to configure the IPX Configuration parameters.

Parameter:	**Configured Network Number (hex)**
Default:	None
Options:	Any valid IPX network address
Function:	Assigns an IPX address to the interface.
Instructions:	Enter the IPX address of the interface in hexadecimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.22

Note: *If you are configuring an IPX interface that will enable IPXWAN, leave this parameter blank. If you are configuring this interface as Unnumbered RIP, you must enter a zero for this parameter.*

If you are attempting to establish a connection to a Series 5 Bay Networks router, or a router that does not implement IPXWAN or PPP, then you must enter a nonzero network address (for example, the network address of the link).

Once you save the contents of the IPX Configuration window, the Configured Network Number appears in the list of IPX interfaces. You can later edit the Configured Network Number parameter in the IPX Interfaces window, which has an option to change certain configured IPX circuit parameters.

Parameter:	**RIP/SAP**
Default:	Depends on whether you selected RIP/SAP along with IPX on the Select Protocols window
Options:	Yes | No
Function:	Indicates whether you have RIP and SAP configured on that interface.
Instructions:	The Configuration Manager sets the default value for this parameter based on your selection in the Select Protocols window. You can, however, change the value of this parameter as long as the IPX Configuration window remains in the workstation display. You can also change the value of this parameter in the IPX Change Circuit window (see Chapter 4).
MIB Object ID:	Not applicable

Parameter:	**Configured Encaps**
Default:	None (media dependent)
Options:	Ethernet | LSAP | Novell | SNAP | PPP
Function:	Specifies the encapsulation methods available for each link layer type (for example, Ethernet or Token Ring).
Instructions:	Select the encapsulation method you need to use. Ensure that the encapsulation method matches that of the clients and servers on the same network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter:	**Circuit Index**
Default:	System assigned
Range:	Any integer within the range of the number of possible circuits
Function:	Assigns a unique identifier to each circuit, usually in order of configuration.
Instructions:	Accept the system-assigned default. If you do change this parameter for a given circuit, the new circuit index replaces the old one, and the other circuit index numbers are unaffected. You cannot enter a value that duplicates another circuit index.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.6

Parameter:	**IPXWAN**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables IPXWAN for this interface. This parameter is active only for circuits that are configured as IPXWAN interfaces.
Instructions:	Select Enable to turn on IPXWAN negotiation for this interface. Select Disable to turn off IPXWAN negotiation for this interface.
MIB Object ID:	Not applicable

Parameter:	**Common Network Number**
Default:	None
Range:	Any valid IPX network number, 0x00000000 through 0xFFFFFFFD, expressed in hexadecimal format
Function:	Specifies the IPX common network number assigned to this IPX circuit. This parameter is active only for circuits that are have IPXWAN enabled.
Instructions:	Enter a valid IPX network number, expressed in hexadecimal format. Do not use the value 0xFFFFFFFE or 0xFFFFFFFF as network numbers. These values are reserved for system use.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.24

Parameter:	**Negotiated Protocol(s)**
Options:	RIP | Unnumbered RIP | NLSP
Function:	Specifies the type of WAN circuit you are enabling.
Instructions:	This parameter is active only for circuits that have the IPXWAN parameter enabled. For a description of RIP and Unnumbered RIP, refer to Chapter 1.
Instructions:	For IPXWAN services, you can enter values into the Negotiated Protocols field as hexadecimal numbers or you can click on Values for a popup menu selection. To enable IPXWAN on the circuit, you can select one or more of the options. Your selection appears on the IPX Configuration window as a hexadecimal number. The values are as follows: 0x00000008 RIP 0x00000010 Unnumbered RIP 0x00000080 NLSP 0x00000018 RIP and Unnumbered RIP 0x00000088 RIP and NLSP 0x00000090 Unnumbered RIP and NLSP 0x00000098 RIP, Unnumbered RIP, and NLSP
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.8

Accepting or Editing the Default Configuration Parameter Values

When you have configured all of the parameters, do one of the following:

- Enable IPX default services. To do this, click on OK. For an IPXWAN circuit, if you click on OK without configuring the negotiated protocols field, IPXWAN will not be enabled. You can, however, enable IPXWAN later. See the description of the Change Circuit option on the IPX Interfaces window in Chapter 4 for details.
- Edit the default values for the circuit. To do this, click on Details. This displays the IPX Configuration window for the circuit (Figure 3-2). Refer to Chapter 4, “Editing IPX Interface Parameters” for appropriate parameter values.

Figure 3-2. IPX Configuration Window for a Specific Interface

Chapter 4
Editing IPX Parameters

Once you have enabled an IPX interface, you can use Site Manager to edit IPX parameters and customize IPX services. Use Site Manager to

- Access IPX parameters
- Edit IPX global parameters
- Edit IPX interface parameters
- Edit IPX RIP interface parameters
- Edit IPX SAP interface parameters
- Add, edit, or delete adjacent hosts
- Add, edit, or delete static routes
- Add, edit, or delete default routes
- Add, edit, or delete NetBIOS static routes
- Add, edit, or delete static services
- Add, edit, or delete route filters
- Add, edit, or delete SAP network-level filters
- Add, edit, or delete SAP server-level filters
- Delete IPX from the router

Note: *The instructions in this chapter assume that you have already configured at least one IPX interface on the router. For information on how to add network interfaces (including IPX interfaces) and on how to configure circuits, see* Configuring Routers.

Accessing IPX Parameters Using the Technician Interface

For each IPX parameter, this chapter provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing set and commit commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: *The Technician Interface does not verify that the value entered is within the range that the router software supports. Entering an invalid value can corrupt your configuration file.*

Site Manager translates the value you enter for an option into a valid MIB value. The Technician Interface does not. For example, when you enable IPX with Site Manager, you select Enable. However, when you enable IPX through the Technician Interface, you *must* specify 1 (Enable) in your **set** command.

To change a configuration setting with Technician Interface, refer to the *WFMIB.asn* file. The Site Manager installation software installs this file into the *\wf\lib* path on the PC or the */usr/wf/lib* path on the UNIX workstation. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Accessing IPX Parameters Using Site Manager

Use Site Manager to select the Configuration Manager tool. You access all IPX parameters from the Configuration Manager window shown in Figure 4-1. (If you select a router model that has eight connectors per slot, the Configuration Manager window shows eight connectors. You may have to enlarge or scroll the window to see all of them.) If you need information about using the Configuration Manager, refer to *Configuring Routers*.

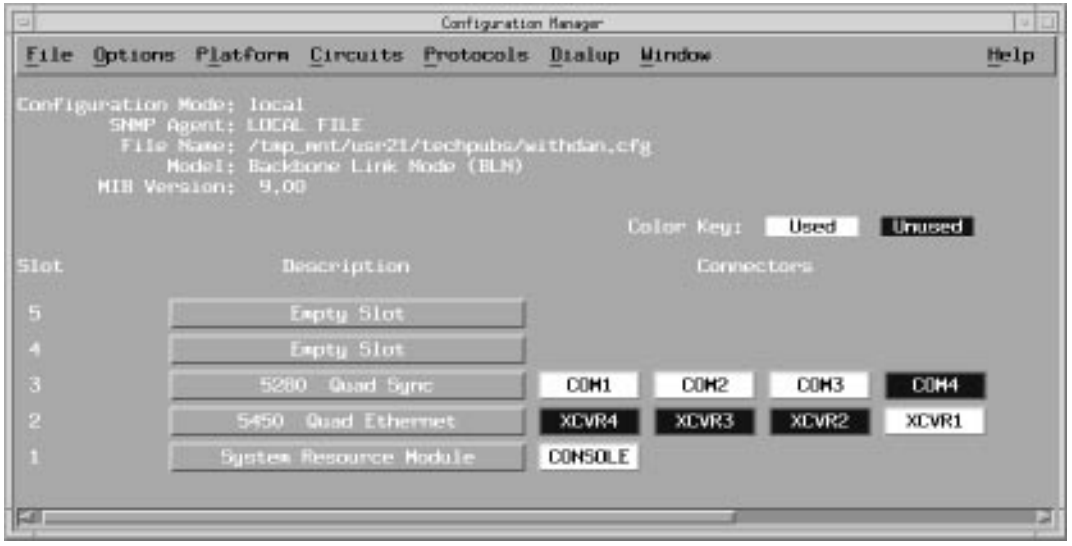

Figure 4-1. Configuration Manager Window

Editing IPX Global Parameters

To edit IPX global parameters, begin at the Site Manager window and from the Tools menu select Configuration Manager. On the Configuration Manager window (Figure 4-1), proceed as follows:

1. **Select the Protocols→IPX→Global option.**

   The Edit IPX Global Parameters window appears (Figure 4-2).

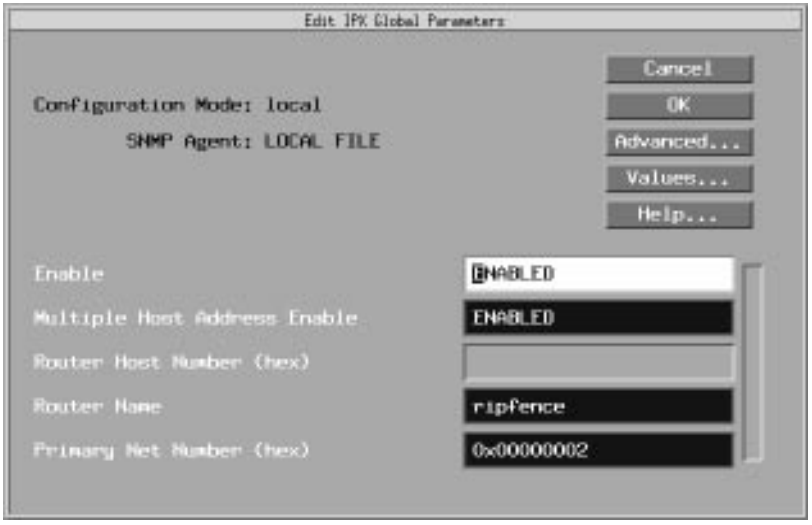

Figure 4-2. Edit IPX Global Parameters Window

2. **Edit those parameters you want to change, according to the following parameter descriptions.**
3. **Click on Advanced. The Edit IPX Advanced Global Parameters window appears.**
4. **Click on OK to exit the window and return to the Configuration Manager window. Save your changes when you are finished.**

IPX Global Parameter Descriptions

This section describes all parameters shown on the Edit IPX Global Parameters window (Figure 4-2).

Parameter: **Enable**

Default: Enable

Options: Enable | Disable

Function: Globally enables or disables the system software mechanisms that allow users to add IPX interfaces to the router configuration:

- Disable — Shuts down all IPX routing for the entire router.
- Enable — Initializes IPX routing for the entire router. Associated IPX interfaces become active, depending on their respective Enable | Disable parameters and on the state of each underlying circuit.

Instructions: Select Disable to disable every IPX interface on the router.

Select Enable to globally reinitialize all IPX interfaces on the router; each interface maintains the most recent setting of its own interface Enable | Disable parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.2

Parameter:	**Multiple Host Address Enable**
Default:	Enable
Options:	Enable | Disable
Function:	If you enable this parameter, an IPX interface can – Use the MAC address located in the PROM on the circuit associated with that interface – Use a MAC address that you enter in the Host Number parameter field for that interface Interfaces on a Token Ring circuit adopt a host ID number based only on the MAC address of the associated circuit. Disabling this parameter causes all IPX interfaces to adopt a single host ID number for the entire host, based either on the serial number of the router backplane or on a number that you enter in the Host Number parameter field.
Instructions:	Choose Enable or Disable, as appropriate for the type of configuration (standard, multiple interfaces per circuit, or multiple circuits per physical segment). See Chapter 2 for a description of each type of configuration.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.15.1.6

Parameter: **Router Host Number (hex)**

Default: If you disable the Multiple Host Address Enable parameter and enter a unique host number, the Configuration Manager assigns this number to all IPX interfaces you configure on the router.

If you disable the Multiple Host Address Enable parameter and do *not* enter a router host ID number for this parameter, the Configuration Manager automatically generates a unique 6-byte host ID number for all IPX interfaces. The generated host ID is based on the serial number of the router's backplane.

Range: Any valid host number

Function: The router either uses this value as a host address for all IPX interfaces, or, if left empty, uses the backplane serial number as the host address for all interfaces (circuits).

Instructions: Enter a value for Router Host Number only if an IPX interface in the router resides on a Token Ring circuit, and both of the following are true:

- You are setting the Token Ring MAC Address Select parameter for that circuit to CNFG.
- You are setting a MAC Address Override value for that circuit.

Do not enter a value for Router Host Number if either of the following is true:

- You want the Configuration Manager to generate a host number automatically.
- An IPX interface on the router resides on a Token Ring circuit, and the Token Ring MAC Address Select parameter is set to BOXWIDE or PROM.

Caution: *The IPX boxwide host address and the Token Ring MAC address must agree when the Multiple Host Address parameter is disabled.*

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.7

Parameter:	**Router Name**
Default:	None
Range:	Any valid NetWare router or server name
Function:	Specifies a symbolic name for the router. Any IPXWAN (RFC1634-compliant) interface in the node uses this name to identify itself to the IPX router or server at the opposite end of the WAN data link. The symbolic name for the router must be unique among those assigned to IPX file servers and routers anywhere in the IPX internetwork.
Instructions:	See the documentation that came with your NetWare operating system for guidelines on specifying a router or server name. It's a good idea to make the name meaningful to users as well as routers.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.15.1.9

Parameter:	**Primary Net Number (hex)**
Default:	None
Range:	The Primary Network Number (PNN) is a string of up to 8 hexadecimal characters. (See the instructions that follow.)
Function:	Specifies an IPX network number for IPXWAN (RFC1634-compliant) link negotiation on all slots. The value of the PNN determines whether the local or remote WAN interface serves as IPX Link Master. The node with the highest PNN value becomes the IPX Link Master. The PNN should be unique among network numbers currently assigned.
Instructions:	Enter a unique network number for each node requiring one or more IPXWAN (RFC1634-compliant) interfaces. (This network number must be unique across the IPX network. Do not enter a number that a server is using as an internal network number, or a number that has been assigned on any segment in the network.) All unused values between 0x00000001 and 0xFFFFFFFD are valid values.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.15.1.5

Editing IPX Advanced Global Parameters

To edit IPX global parameters, click on Advanced in the Edit IPX Global Parameters window. You can also begin at the Site Manager window and from the Tools menu select Configuration Manager. On the Configuration Manager window (refer to Figure 4-1), select the **Protocols→IPX→Global** option. When the Edit IPX Global Parameters window appears, click on Advanced.

1. **In response to either of these actions, the Edit IPX Advanced Global Parameters window appears (Figure 4-3 and Figure 4-4). You have to scroll the parameter list to see the remaining fields on this window.**
2. **Edit the parameters that you want to change.**
3. **Click on OK to exit the window and return to the Configuration Manager window. Save your changes when you are finished.**

Figure 4-3. Edit IPX Advanced Global Parameters Window (Top)

You must scroll to see the last fields in this window. Figure 4-4 shows the bottom of the Edit IPX Advanced Global Parameters window.

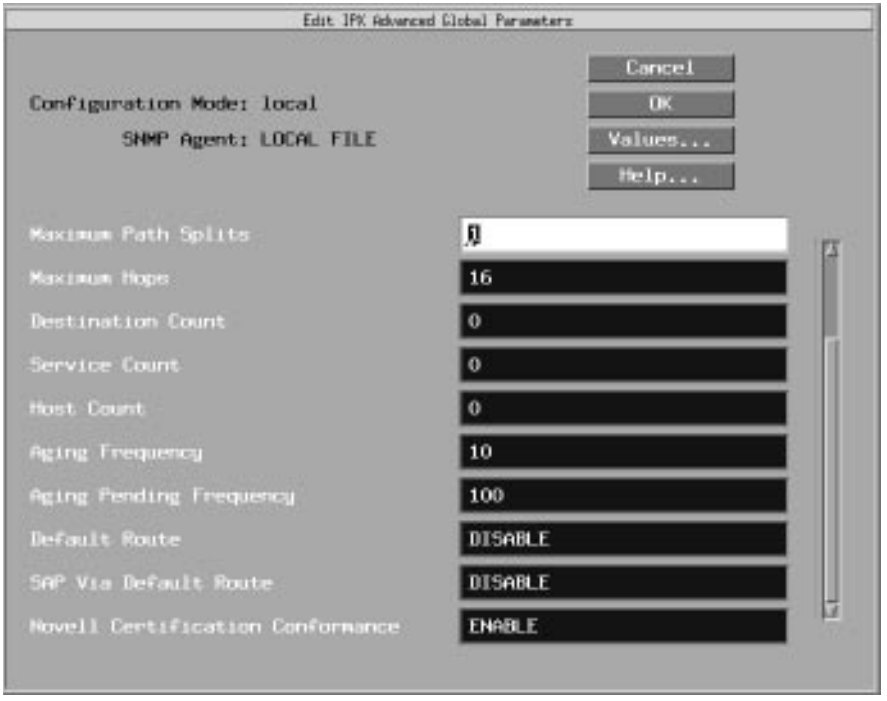

Figure 4-4. Edit IPX Advanced Global Parameters Window (Bottom)

IPX Advanced Global Parameter Descriptions

This section describes all parameters shown on the Edit IPX Advanced Global Parameters window (Figure 4-3 and Figure 4-4).

Parameter: **Routing Method**

Default: Tick

Options: Hop | Tick

Function: Specifies for all slots the method of making IPX "best-route" decisions by:

- Ticks — The amount of time, expressed in ticks, that a packet requires to reach another network segment. (Each tick = 1/18th of a second.)
- Hops — The number of router hops a packet must traverse to reach another network segment.

If you accept the default, Tick, and the router knows about two paths to a network, and both paths have equal tick values, the router chooses the path with the smallest number of hops.

If you select Hop, and the best route results in the same number of hops, the router makes its decision based only on hops.

Instructions: Choose the method that results in the best routing performance. Usually, the best route is the one with:

- The lowest number of ticks for a packet to reach a node on the destination network
- The lowest number of hops (if multiple routes exist with equal numbers of ticks for a packet to reach a node on the destination network)

If routes exist with equal numbers of ticks and hops, choose either method. We recommend using the default (tick-based) method, because tick-based routing takes into account actual link delay in determining the best path between IPX networks. Thus, it provides a more accurate routing mechanism than simply "hop count."

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.3

Parameter:	**Maximum Paths**
Default:	1 (path)
Range:	1 to 5 (paths)
Function:	Specifies the maximum number of equal-cost paths allowed for a given network destination and routing method.
Instructions:	Accept the default (1) or specify an integer in the range 1 to 5.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.5

Parameter:	**Log Filter**
Default:	Trace
Options:	None | Debug | Info | Trace | Debug Info | Debug Trace | Info Trace | Debug Info Trace
Function:	Filters out the specified type of log message. For example, the default setting (Trace) filters out trace messages.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user. Changing the value of this parameter produces significant boxwide effects on memory allocation within the router, and these changes can significantly affect router performance. If you are qualified as an expert user, enter a filtering mode that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.4

Parameter:	**Maximum Path Splits**
Default:	1 (path)
Range:	1 to 5 (paths)
Function:	Specifies the maximum number of equal-cost paths over which IPX will do load balancing to a particular destination. For example, if the maximum path splits equals 5, and there are five equal-cost routes to a destination, IPX will distribute the packets over the five paths in a round-robin fashion.
Instructions:	Accept the default (1) or specify an integer in the range 1 to 5.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.6

Parameter:	**Maximum Hops**
Default:	16 (hops)
Range:	1 to 255 (hops)
Function:	Specifies the maximum number of hops an IPX packet may take to reach its destination.
Instructions:	Accept the default, 16, or specify an integer in the range 1 to 255. In the case of RIP, every node in the network should use the same Maximum Hops parameter value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.7

Parameter:	**Destination Count**
Default:	0
Range:	0 to 5000 (destinations)
Function:	Specifies the maximum number of destinations (networks) that the user expects the router to learn. IPX uses this value to preallocate table sizes for forwarding and network tables. If you specify zero, the default value, IPX dynamically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.17

Parameter:	**Service Count**
Default:	1 (service)
Range:	1 to 5000 (services)
Function:	Indicates the maximum number of services that the user expects the router to learn. IPX uses this value to preallocate table sizes for service tables. If you specify zero, the default value, IPX automatically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.19

Parameter:	**Host Count**
Default:	1 (host)
Range:	1 to 5000 (hosts)
Function:	Indicates the maximum next-hop hosts that the user expects the router to learn. IPX uses this value to preallocate table sizes for host tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.21

Parameter:	**Aging Frequency**
Default:	10 (seconds)
Range:	1 to the maximum positive integer (seconds)
Function:	Specifies the granularity, in seconds, for aging RIP and SAP information. IPX checks whether any routes have timed out every *n* seconds, where *n* is the interval that this parameter specifies.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.23

Parameter:	**Aging Pending Frequency**
Default:	100 (routes and services)
Range:	1 to maximum positive integer (routes and services)
Function:	Specifies the number of routes and services to age (process) before pending. A higher number lets the aging process proceed more quickly.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.24

Parameter:	**Default Route**
Default:	Disable
Options:	Enable | Disable
Function:	Globally enables or disables the use of the default route 0xFFFFFFFE for IPX routing. Enable — Directs the router to use the default route (if one exists in its routing table) when it receives an IPX packet that does not contain a known IPX destination address within the IPX protocol header. Disable — Forces the router to drop a packet whose destination address is unknown, even if a default route exists.
Instructions:	Select Enable to allow IPX default routing. Select Disable to turn off default routing.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.25

Parameter:	**SAP Via Default Route**
Default:	Disable
Options:	Enable | Disable
Function:	Indicates whether a SAP advertisement can be learned from an interface if the network number advertised in the SAP advertisement is unreachable, but a default route is accessible from that interface. Enable — Directs the router to accept a service if a direct or default route to the server is known. Disable — Accepts a service only if a direct route to the server advertising the service is known.
Instructions:	This feature gives you the option of making SAP entries available if the IPX default route is reachable. Select Enable to enable IPX default routing globally for SAP advertisements. Select Disable to turn off default SAP advertisement routing.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.26

Note: *Since it deviates from the IPX Default Route specification, enabling this feature may cause the interface to be incompatible with other router implementations.*

Parameter:	**Novell Certification Conformance**
Default:	Enable
Options:	Enable | Disable
Function:	Indicates whether you want the router to conform to Novell NetWare standards by propagating a NetBIOS Type 20 packet out of all its interfaces.
Instructions:	Accept the default, Enable, if you want the router to propagate NetBIOS Type 20 packets out of all its interfaces (conforming to Novell standards). Select Disable if you have NetBIOS static routes configured and you want the router to direct a packet to its destination network. You must set the same option (Enable or Disable) for all routers in the network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.15

Editing IPX Interface Parameters

Any IPX interface you add to a physical circuit inherits a default set of IPX parameter values from the global/slotwide IPX process. You can use the Configuration Manager to access and further modify or customize parameters belonging to a specific interface. To do so, begin at the Configuration Manager window (refer to Figure 4-1) and proceed as follows:

1. **Select the Protocols→IPX→Interfaces option to display the IPX Interfaces window (Figure 4-5). You must scroll the parameter list to see all the fields.**

Figure 4-5. IPX Interfaces Window

The IPX Interfaces window lists each IPX interface entry in the router configuration as follows:

<circuit_name>, <circuit_index>, <network_number>

Other entries on this line indicate whether IPXWAN is enabled and whether RIP or SAP is on.

2. **Select the interface you want to modify. The parameters associated with that interface appear in the parameter value window.**
3. **Edit those parameters you want to change. Click on Apply to implement your changes.**
4. **Use the scroll bar to display the remaining parameters.**
5. **Click on Done to save your changes and exit the window.**

IPX Interface Parameter Descriptions

This section describes how to set all parameters shown on the IPX Interfaces window (Figure 4-5).

Parameter: **Enable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables IPX routing on this interface.

Enable — Initializes the IPX interface you added to a circuit. You can also use the Enable setting to reinitialize an existing disabled IPX interface. The actual operating state of an interface, once enabled, depends on

– The current state of the associated circuit

– The current state of the IPX global/slotwide protocol process

Disable — Forces an IPX interface into the down (inoperative) state.

Instructions: Select Enable if you previously set this parameter to Disable and now want to re-enable IPX routing on this interface.

Select Disable only if you want to disable IPX routing on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.2

Parameter: **Name**

Default: None

Range: Any valid IPX server name

Function: Specifies a symbolic name for the interface.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a host, interface, router, or server name. It's a good idea to make the name meaningful to users as well as to routers.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.7

Parameter:	**Cost**
Default:	1 (for hop- or tick-based routing)
Range:	1 to the maximum positive integer (if tick-based routing is enabled) 1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)
Function:	Sets the cost (number of ticks or hops) for this interface. The cost is added to route information learned on this interface through RIP and is included in subsequent RIP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.38

Parameter: **Host Number**

Default: None

Range: Any valid IPX host ID number

Function: If you enable Multiple Host Address Enable and want to accept the PROM-based default setting for the MAC Address Select circuit parameter, this IPX interface adopts a host number based on the MAC address of the underlying circuit. In this case, a PROM on the circuit supplies the number for the MAC address of the circuit and the host number of the interface.

You can enter a host number for this interface when:

- Multiple Host Addressing is enabled
- You do not want to accept the PROM-based (default) setting for MAC Address Select
- The circuit type supports only selective mode of operation (such as with Ethernet circuits)

If you enter a host number, the circuit adopts that value as the MAC address at which this interface can receive frames. (The MAC address configured at the circuit/line level remains effective for all other interfaces configured on the same circuit.)

You can enter a host number for this interface when the underlying circuit is Token Ring; see the instructions that follow.

Site Manager does not let you enter an IPX host number for any IPX interface if you first disable Multiple Host Address Enable in the IPX Global Parameters window.

Instructions: Enter a value only if the circuit is not Token Ring and you want to assign a host number that is unique within the IPX internetwork to this IPX interface.

To set the host number of an IPX interface on a Token Ring circuit, you must change the MAC Address Select parameter for that circuit to CNFG (user-configured) and enter a MAC Address Override value for the circuit. The interface uses that value as its host number. This changes the circuit MAC address for all protocols configured on that Token Ring circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.25

Parameter:	**Configured Encaps**
Default:	Circuit medium dependent
Options:	Circuit medium dependent (see Instructions) Possible values: Ethernet | LSAP | Novell | SNAP | PPP
Function:	Specifies the encapsulation methods (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, Token Ring, or sync). The encapsulation method supports communication on a specific logical network.
Instructions:	Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows: – Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames. – Token ring circuits support LSAP and SNAP frames. – Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames. – FDDI circuits support LSAP and SNAP frames. – HSSI circuits support PPP and SNAP Frames. – ISDN circuits support PPP frames.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter:	**TR End Station**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables source routing on this interface. This parameter appears only when you add an IPX interface on a Token Ring circuit.
Instructions:	Select Enable if this interface connects to a bridged Token Ring network. Select Disable only if you want to disable source routing over this interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.59

Parameter:	**NetBIOS Accept**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables acceptance of all NetBIOS Type 20 (broadcast) packets received by this interface from an external source.
Instructions:	Select Enable if you want this interface to accept all NetBIOS broadcast packets from an external source. Select Disable only if you want this interface to reject all NetBIOS broadcast packets from an external source.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.60

Parameter:	**NetBIOS Deliver**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables outbound delivery of all NetBIOS Type 20 (broadcast) packets received by this interface from another interface.
Instructions:	Select Enable if you want to re-enable outbound delivery of NetBIOS broadcast packets received internally. Select Disable only to drop NetBIOS broadcast packets received internally.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.61

Parameter:	**Broadcast Address (hex)**
Default:	0xFFFFFFFFFFFF (not displayed)
Options:	Default value or a user-specified WAN broadcast address.
Function:	Specifies a broadcast address for this IPX interface. (This parameter is available for any WAN protocol and any media type.)
Instructions:	The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a WAN broadcast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol. Leave blank to accept the default value or enter a WAN broadcast address to send all broadcast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all broadcast traffic through all logical connections associated with the IPX interface you are configuring. Broadcast traffic includes RIP and SAP broadcasts.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.28

Parameter:	**Multicast Address (hex)**
Default:	0xFFFFFFFFFFFF (not displayed)
Options:	Default value or a user-specified WAN multicast address.
Function:	Specifies a multicast address for this IPX interface. (This parameter is available for any WAN protocol and any media type.) The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a multicast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.
Instructions:	Leave blank to accept the default value or enter a WAN multicast address to send all multicast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all multicast traffic through all logical connections associated with the IPX interface you are configuring.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.30

Parameter:	**IPX Watchdog Spoofing**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether a router can respond locally to broadcast IPX watchdog packets on behalf of clients that use dial-in connections.
Instructions:	Enable local watchdog packet acknowledgment to improve the efficiency of IPX wide-area links.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.64

Parameter:	**Delay**
Default:	0
Range:	0-2147483647
Function:	Specifies the length of time, in microseconds, required to transmit 1 byte of data (excluding protocol headers) to a destination on the other end of this IPX circuit if the circuit is free of other traffic.
Instructions:	Enter a value between 0 and 2147483647.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.66

Parameter:	**Throughput**
Default:	0
Range:	0-2147483647
Function:	Specifies the amount of data, in bits per second, that can flow through an IPX circuit if the circuit is free of other traffic.
Instructions:	Enter a value between 0 and 2147483647.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.67

Editing IPX Change Circuit Parameters

Any IPX interface you add to a physical circuit inherits a default set of IPX parameter values from the global/slotwide IPX process. You can use the Configuration Manager to access and further modify or customize parameters belonging to a specific interface, or to change certain parameter values that you previously configured.

To edit the configurable parameters of an IPX interface, begin at the Configuration Manager window (Figure 4-1) and proceed as follows:

1. **Select Protocols→IPX→Interfaces. On the IPX Interfaces subwindow, select the circuit for which you want to edit the parameters.**
2. **Click on Change. The IPX Change Circuit window appears (Figure 4-6).**

   The window displays the parameters you can change for this circuit, with the identifier of the circuit at the top of the window.

Figure 4-6. IPX Change Circuit Window

Note: *The Configured Network Number parameter is active only for circuits that are not configured as IPXWAN interfaces. The IPXWAN, Common Network Number, and Negotiated Protocols parameters appear only when the circuit is configured as an IPXWAN interface.*

3. **Click on any parameter value you want to change; then enter a new value (or click on Values and select one from the popup window).**
4. **Click on OK to save your changes and exit the IPX Change Circuit window.**

IPX Change Circuit Parameter Descriptions

This section describes how to set all parameters shown on the IPX Change Circuit window (refer to Figure 4-6.). The IPX circuit identifier appears in the window title.

Parameter:	**Configured Network Number (hex)**
Default:	None
Range:	Any valid IPX network number in hexadecimal format
Function:	Identifies the IPX network number that the user assigned to this IPX circuit. This parameter is active only for circuits that are not configured as IPXWAN interfaces or for those with the IPXWAN parameter explicitly disabled.
Instructions:	Enter a valid IPX network number in hexadecimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.22

Parameter:	**Configured Encaps**
Default:	Circuit medium dependent
Options:	Circuit medium dependent (see Instructions) Possible values: Ethernet | LSAP | Novell | SNAP | PPP
Function:	Specifies the encapsulation methods (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, Token Ring, or sync). The encapsulation method supports communication on a specific logical network.
Instructions:	Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows: – Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames. – Token ring circuits support LSAP and SNAP frames. – Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames. – FDDI circuits support LSAP and SNAP frames. – HSSI circuits support PPP and SNAP frames. – ISDN circuits support PPP frames.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter:	**Circuit Index**
Default:	System-assigned
Range:	Any valid circuit identifier
Function:	Uniquely identifies this circuit within this instance of IPX.
Instructions:	Accept the default or enter a valid circuit identifier.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.6

Parameter:	**IPXWAN**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables IPXWAN for this interface on this router. This parameter is active only for circuits that are configured as IPXWAN interfaces.
Instructions:	Select Enable to turn on IPXWAN negotiation for this interface. Select Disable to turn on IPXWAN negotiation for this interface.
MIB Object ID:	Not Applicable

Parameter:	**Common Network Number (hex)**
Default:	None
Range:	Any valid IPX network number, 0x00000000 to 0xFFFFFFFD in hexadecimal format
Function:	Specifies the IPX common network number assigned to this IPX circuit. This parameter is active only for circuits that are configured as IPXWAN interfaces that have the IPXWAN parameter enabled.
Instructions:	Enter a valid IPX network number in hexadecimal format. Do not use the values 0xFFFFFFFE or 0xFFFFFFFF as network numbers. These values are reserved for system use.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.24

Parameter:	**Negotiated Protocol(s)**
Default:	Unnumbered RIP
Options:	RIP | Unnumbered RIP | NLSP
Function:	Indicates the protocol negotiated for this interface. This parameter is active only for circuits that are configured as IPXWAN interfaces and that have the IPXWAN parameter enabled.
Instructions:	Accept the default or click on Values to display the other choices. You can select more than one option. Click on the options you prefer, then click on OK to accept your choices. The parameter value appears as a hexadecimal number on the IPX Change Circuit window. The values are as follows: 0x00000008 RIP 0x00000010 Unnumbered RIP 0x00000080 NLSP 0x00000018 RIP and Unnumbered RIP 0x00000088 RIP and NLSP 0x00000090 Unnumbered RIP and NLSP 0x00000098 RIP, Unnumbered RIP, and NLSP
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.8

Editing IPX RIP Circuit Parameters

If RIP is enabled on an IPX circuit, you can edit the RIP parameters of that circuit by accessing the IPX RIP Circuit window for that circuit. For instructions on how to add an IPX RIP interface to a circuit, refer to *Configuring Routers*.

To edit the configurable RIP parameters of an IPX interface, begin at the Configuration Manager window (refer to Figure 4-1) and proceed as follows:

1. **Select the Protocols→IPX→Interfaces options. On the IPX Interfaces subwindow, select the circuit for which you want to edit the RIP parameters.**
2. **Click on RIP. The IPX RIP Circuit window appears (Figure 4-7 and Figure 4-8).**

   The window displays the parameters you can change for this RIP circuit.

3. **Click on any parameter value you want to change; then enter a new value (or click on Values and select one from the popup window).**
4. **Click on OK to save and exit the IPX RIP Circuit window.**

Figure 4-7. IPX RIP Circuit Window (Top)

You have to scroll to see the fields at the bottom of the window (Figure 4-8).

Figure 4-8. IPX RIP Circuit Window (Bottom)

IPX RIP Circuit Parameter Descriptions

This section describes how to set all parameters shown on the IPX RIP Circuit window (refer to Figure 4-7). The IPX circuit identifier appears in the window title.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether RIP is enabled on this IPX circuit.
Instructions:	Select Enable to enable RIP on this circuit. Select Disable to disable RIP on this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.2

Note: *If this parameter is set to Enable, a route filter can still prohibit the interface from updating its internal routing tables. See the description of route filtering in this chapter.*

Parameter:	**Mode**
Default:	Listen/Supply
Options:	Listen/Supply | Listen | Supply
Function:	Specifies the mode for this circuit.
Instructions:	Select one of the following values: Listen/Supply — specifies that this interface both listens for and supplies RIP updates, as described in the following items. Listen — specifies whether this interface listens to RIP Periodic and Triggered updates from neighboring networks and conveys received routing information to its internal routing table. Supply — specifies whether the interface transmits all RIP Periodic and Triggered updates to routers in neighboring networks.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.6

Parameter:	**Pace**
Default:	18
Range:	0 to 1000
Function:	Specifies the maximum pace (in packets per second) at which RIP packets can be sent on this circuit. A value of zero means that there is no limit on the pace.
Instructions:	Accept the default or specify an integer value up to 1000.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.7

Parameter:	**Update Interval (sec)**
Default:	60
Range:	0 to 2678400
Function:	Adjusts the frequency of RIP update packet transmissions, in seconds, for this circuit.
Instructions:	The higher the number you enter, the less frequent the transmissions. If you enter zero, no periodic RIP updates are sent out over the IPX interface to the router. However, RIP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.8

Parameter:	**Age Multiplier**
Default:	3 (update interval increments)
Range:	1 to 6 (increments)
Function:	Specifies the holding multiplier as the number of update intervals for information received in RIP periodic updates.
Instructions:	Accept the default value or specify a value in the range 1 to 6. Increasing this value can cause routes to take longer to age out. Decreasing it could cause the router to age routes prematurely, if routing updates are missed. The combination of the update interval and age multiplier should be the same for all systems on a network segment.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.9

Parameter:	**Packet Size**
Default:	432
Options:	Circuit-type dependent
Function:	Specifies the maximum RIP packet size, in bytes, used on this circuit.
Instructions:	Accept the default (432 bytes) unless you have a specific reason for specifying a different size packet. The packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.10

Parameter:	**Use Multicast**
Default:	Yes
Options:	Yes | No
Function:	Specifies whether to use a multicast address, configured with the Multicast Address parameter, to send RIP packets.
Instructions:	Accept the default to allow multicast transmission of RIP packets. Select No to disable multicast transmission of RIP packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.14

Parameter:	**Split Horizon**
Default:	Enable
Options:	Enable | Disable
Function:	When generating RIP updates to be transmitted from an interface, the interface can exclude RIP routes learned on that interface.
Instructions:	Select Enable if you previously set this parameter to Disable and now do not want the router to transmit RIP updates received from the interface over that same interface. Select Disable only if you want the router to transmit RIP updates received from the interface over that same interface. Routes learned on that interface will be included in the RIP updates generated for that interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.15

Parameter:	**Immediate Update**
Default:	Enable
Options:	Enable | Disable
Function:	When a change in status occurs for this circuit, immediately propagate that information to other routers in the internetwork.
Instructions:	Accept the default. Enabling this parameter facilitates network traffic by letting routers know immediately about new or failed routes. When this parameter is disabled, other routers learn about such changes only at the next periodic update interval.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.17

Parameter:	**Default Route Supply**
Default:	Enable
Options:	Enable | Disable
Function:	If a default route exists in the routing table, this parameter specifies whether to advertise the default route, 0xFFFFFFE, in RIP packets.
Instructions:	Select Enable to enable default route supply (that is, to advertise the default route) on this circuit. Select Disable to disable default route supply (that is, not advertise the default route) on this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.18

Parameter:	**Default Route Listen**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether to accept the default route, 0xFFFFFFE, in RIP packets received on this circuit.
Instructions:	Select Enable to accept the default route in RIP packets on this circuit. Select Disable to reject the default route in RIP packets on this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.32.1.19

Editing IPX SAP Circuit Parameters

If SAP is enabled on an IPX circuit, you can edit the SAP parameters of that circuit by accessing the IPX SAP Circuit window for that circuit. For instructions on how to add an IPX SAP interface to a circuit, refer to *Configuring Routers*.

To edit the configurable SAP parameters of an IPX interface, begin at the Configuration Manager window (refer to Figure 4-1) and proceed as follows:

1. **Select the Protocols→IPX→Interfaces options. On the IPX Interfaces subwindow, select the circuit for which you want to edit the SAP parameters.**
2. **Click on SAP. The IPX SAP Circuit window appears (Figure 4-9).**

   The window displays the parameters you can change for this SAP circuit.

Figure 4-9. IPX SAP Circuit Window (Top)

3. **Click on any parameter value you want to change; then enter a new value (or click on Values and select one from the popup window).**
4. **Click on OK to save and exit the IPX SAP Circuit window.**

IPX SAP Circuit Parameter Descriptions

This section describes how to set all parameters shown on the IPX SAP Circuit window (Figure 4-9). The IPX circuit identifier appears in the window title.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether SAP is enabled on this IPX circuit.
Instructions:	Select Enable to enable SAP on this circuit. Select Disable to disable SAP on this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.2

Note: *If this parameter is set to Enable, a SAP filter can still prohibit the interface from updating its internal SAP tables. See the description of SAP filtering in Chapter 1.*

Parameter:	**Mode**
Default:	Listen/Supply
Options:	Listen/Supply | Listen | Supply
Function:	Specifies the mode for this circuit.
Instructions:	Select one of the following values: *Listen/Supply* — specifies that this interface both listens for and supplies SAP updates, as described in the following items. *Listen* — specifies whether this interface listens to SAP Periodic and Triggered updates from neighboring networks and conveys received SAP services information to its internal SAP services table. *Supply* — specifies whether the interface transmits all SAP Periodic and Triggered updates to routers in neighboring networks.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.6

Parameter:	**Pace**
Default:	18
Range:	0 to 1000
Function:	Specifies the maximum pace (in packets per second) at which SAP packets can be sent on this circuit. A value of zero means that there is no limit on the pace.
Instructions:	Accept the default or specify an integer value up to 1000.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.7

Parameter:	**Update Interval (sec)**
Default:	60
Range:	0 to 2678400
Function:	Adjusts the frequency, in seconds, of SAP update packet transmissions for this circuit.
Instructions:	The higher the number you enter, the less frequent the transmissions. If you enter zero, no periodic updates are sent out over the IPX interface to the router. However, SAP immediate (one-time) updates still propagate through the network, in compliance with Novell standards.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.8

Parameter:	**Age Multiplier**
Default:	3 (update interval increments)
Range:	1 to 6 (increments)
Function:	Specifies the holding multiplier, in update interval increments, for information received in SAP periodic updates.
Instructions:	Accept the default value or specify a value in the range 1 to 6. Increasing this value can cause routes to take longer to age out. Decreasing it could cause the router to age routes prematurely, if routing updates are missed. The combination of the update interval and age multiplier should be the same for all systems on a network segment.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.9

Parameter:	**Packet Size**
Default:	480
Options:	Circuit-type dependent
Function:	Specifies the maximum SAP packet size, in bytes, used on this circuit.
Instructions:	Accept the default (480 bytes) unless you have a specific reason for specifying a different size packet. The packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.10

Parameter:	**Nearest Server Reply**
Default:	Yes
Options:	Yes | No
Function:	Specifies whether to respond to SAP *get_nearest_server* requests.
Instructions:	Accept the default to allow this router to respond to a SAP *get_nearest_server* request. If you have disabled split horizon, you may want to set this parameter to No.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.11

Parameter:	**Use Multicast**
Default:	Yes
Options:	Yes | No
Function:	Specifies whether to use a multicast address to send SAP packets.
Instructions:	Accept the default to allow multicast transmission of SAP packets. Select No to disable multicast transmission of SAP packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.16

Parameter:	**Split Horizon**
Default:	Enable
Options:	Enable | Disable
Function:	When generating SAP updates to be transmitted from an interface, the interface can exclude SAP servers learned on that interface.
Instructions:	Select Enable if you previously set this parameter to Disable and now do not want the router to transmit SAP updates received from the interface over that same interface. Select Disable only if you want the router to transmit SAP updates received from the interface over that same interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.17

Parameter:	**Immediate Update**
Default:	Enable
Options:	Enable | Disable
Function:	When a change in status occurs for this circuit, immediately propagate that information to other routers in the internetwork.
Instructions:	Accept the default. Enabling this parameter facilitates network traffic by letting routers know immediately about new or failed services. When this parameter is disabled, other routers learn about such changes only at the next periodic update interval.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.33.1.19

Using NetBIOS Static Routes

The NetBIOS Static Route function lets you reduce NetBIOS network traffic by configuring a NetBIOS static route to a NetBIOS service name. The IPX router then restricts broadcast NetBIOS packets, which are usually forwarded to all network interfaces on a single network.

You can add, edit, and delete NetBIOS static routes to other networks, regardless of the routers used in those networks. You perform these functions from the IPX NetBIOS Static Routes window. Begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→NetBIOS Static Routes** option. The IPX NetBIOS Static Routes window appears (Figure 4-10).

Figure 4-10. IPX NetBIOS Static Routes Window

The IPX NetBIOS Static Routes window displays each NetBIOS Static Route entry in the router configuration by name.

Refer to the following sections to add, edit, and delete NetBIOS static routes.

Adding a NetBIOS Static Route

To add a NetBIOS static route, begin at the IPX NetBIOS Static Routes window (refer to Figure 4-10) and proceed as follows:

1. **Click on Add.**
2. **The IPX NetBIOS Static Route Configuration window appears (refer to Figure 4-11).**

Figure 4-11. IPX NetBIOS Static Route Configuration Window

3. **Enter values for the Target Network and Target Server parameters, using the parameter descriptions that follow as guidelines.**
4. **Click on OK to save your entries.**

The IPX NetBIOS Static Routes window (refer to Figure 4-10) reappears immediately after you click on OK.

IPX NetBIOS Static Route Configuration Parameter Descriptions

This section describes all parameters shown in the IPX NetBIOS Static Route Configuration window.

Parameter:	**Target Server**
Default:	None
Options:	The name of a NetBIOS target server, specified as a string of up to 16 alphanumeric characters (which can include wildcards and pattern-matching characters). You can include any printable character, including $, #, and so on. To specify a backslash, enter two backslashes (\\). You can also use the hexadecimal equivalent (*xx*) of any valid ASCII character. For example, you can specify \20 for space or \21 for ! (note that *xx* counts as one character).
Function:	Specifies the name of the NetBIOS server.
Instructions:	Enter the name or part of the name of the NetBIOS server. The name can be up to 16 alphanumeric characters. For a list of the wildcards and pattern-matching characters, refer to Table 4-1 on page 4-78.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.27.1.4

Note: *The Configuration Manager does not let you reconfigure the Target Server parameter for a static route. If you want to change this parameter, you must delete the static route and add a new route. However, you can reconfigure all other parameters associated with a static route.*

Parameter:	**Target Network (hex)**
Default:	None
Range:	Any valid network address in hexadecimal notation
Function:	Specifies the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.
Instructions:	Enter a network address of up to 8 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.27.1.5

Editing a NetBIOS Static Route

You can edit the configurable parameters of a NetBIOS static route in the node configuration.

To edit the configurable parameters associated with an existing NetBIOS static route, begin at the Configuration Manager window (Figure 4-1) and select the **Protocols→IPX→NetBIOS Static Routes** option. The IPX NetBIOS Static Routes window appears as shown in Figure 4-10. From this window, proceed as follows:

1. **Select the NetBIOS static route you want to edit by clicking on the appropriate entry in the list of static routes.**
2. **Click on any parameter value you want to change; then enter a new value.**
3. **Click on OK to exit the IPX NetBIOS Static Routes window and return to the Configuration Manager window.**

IPX NetBIOS Static Route Parameter Descriptions

This section describes how to set all parameters shown on the IPX NetBIOS Static Routes window (refer to Figure 4-10).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies the state (active or inactive) of the static route record in the NetBIOS routing table.
Instructions:	Select Disable to make the static route record inactive in the NetBIOS routing table. Select Enable to make the static route record active in the NetBIOS routing table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.27.1.2

Parameter:	**Target Network (hex)**
Default:	None
Range:	Any valid network address in hexadecimal notation
Function:	Specifies the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.
Instructions:	Enter a network address of up to 8 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.27.1.5

Deleting a NetBIOS Static Route

To delete an IPX NetBIOS static route:

1. **Select from the IPX NetBIOS Static Routes window the static route you want to delete from the node configuration.**
2. **Click on Delete in the NetBIOS Static Routes window (refer to Figure 4-10).**

The system software deletes the NetBIOS static route entry you selected, and the entry disappears from the list of static routes in the IPX NetBIOS Static Routes window.

Editing Adjacent Host Parameters

The following sections show you how to add, edit, and delete adjacent hosts in a Bay Networks router configuration. You perform these actions through the IPX Adjacent Hosts window.

To access the IPX Adjacent Hosts window, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. The IPX Static Interface Tables Configuration window appears (Figure 4-12).

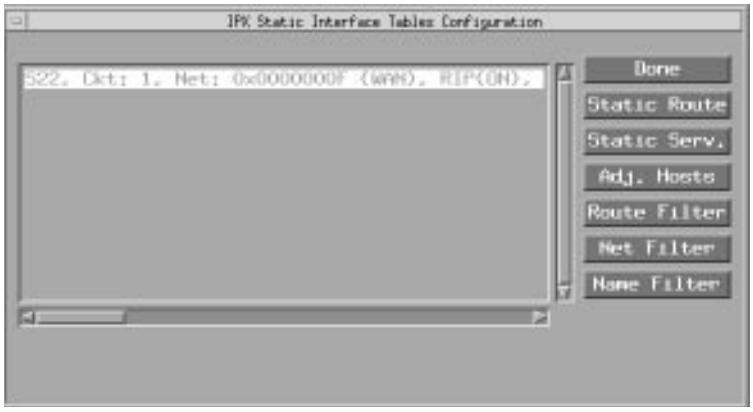

Figure 4-12. IPX Static Interface Tables Configuration Window

Select the interface for which you want to configure the adjacent hosts. Click on Adj. Hosts. The IPX Adjacent Hosts window appears (Figure 4-13), showing a list of all adjacent hosts currently defined in the router configuration.

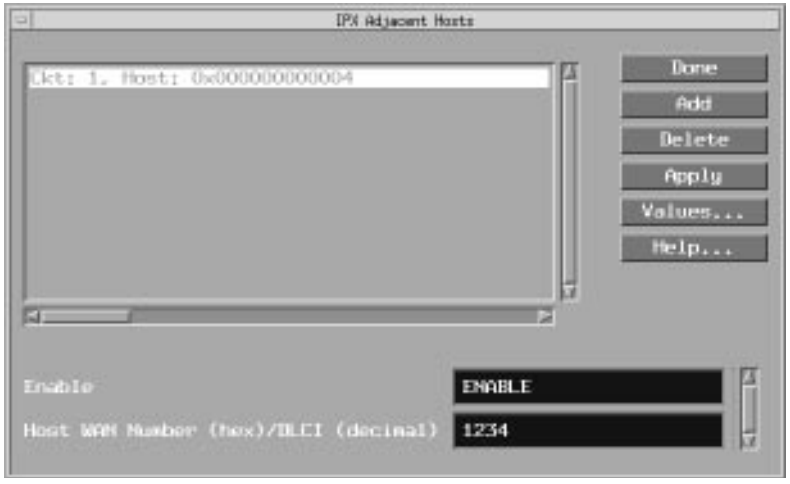

Figure 4-13. IPX Adjacent Hosts Window

The IPX Adjacent Hosts window displays each Adjacent Host entry in the router configuration, as follows:

<circuit_ID>, <host_number>

Adding an Adjacent Host

To add an adjacent host, begin at the IPX Adjacent Hosts window (refer to Figure 4-13) and proceed as follows:

1. **Click on Add.**

   The IPX Adjacent Host Configuration window appears (Figure 4-14).

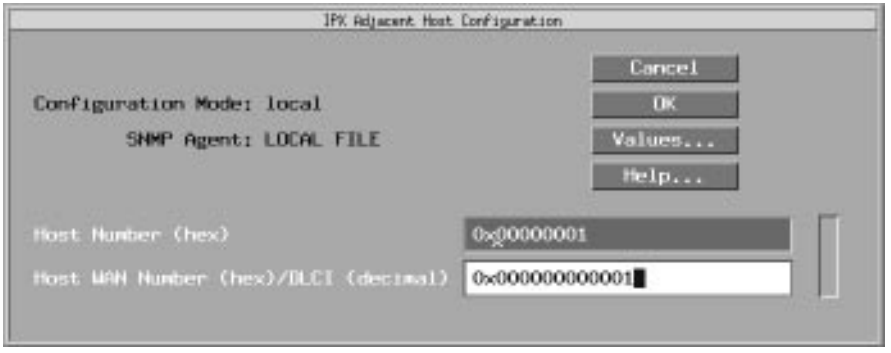

Figure 4-14. IPX Adjacent Host Configuration Window

2. **Enter values for the Host Number (hex) and Host WAN Number (hex)/DLCI (decimal) address parameters.**
3. **Click on OK to save your entries to the configuration file.**

The IPX Adjacent Hosts window (Figure 4-13) reappears immediately after you press OK.

Adjacent Host Configuration Parameter Descriptions

This section describes all parameters shown on the IPX Adjacent Host Configuration window (refer to Figure 4-14).

Parameter:	**Host Number (hex)**
Default:	None
Options:	Valid host ID of the adjacent host
Function:	Specifies the host ID of the adjacent host.
Instructions:	Enter a host ID of up to 12 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.26.1.5

Parameter:	**WAN Address (hex)/DLCI (decimal)**
Default:	None
Options:	WAN Address | Data Link Connection Identifier
Function:	Lets you enter a WAN address or a DLCI. The format depends on the underlying data link protocol type.
Instructions:	Enter a WAN address of up to 16 hexadecimal characters if the interface is on an ATM or SMDS network Enter a decimal DLCI number if the interface is on a Frame Relay network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.26.1.6

Editing an Adjacent Host

You can edit the configurable parameters of an Adjacent Host entry in the node configuration. To edit the configurable parameters associated with an existing adjacent host, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option and click on Adjacent Hosts. The IPX Adjacent Hosts window appears, as shown in Figure 4-13. From this window, proceed as follows:

1. **Select the adjacent host you want to edit by clicking on the appropriate entry in the list of adjacent hosts.**
2. **Click on any parameter value you want to change; then enter a new value.**
3. **Click on OK to save and exit the IPX Adjacent Hosts window.**

IPX Adjacent Hosts Parameter Descriptions

The parameters listed in the IPX Adjacent Hosts window (Figure 4-13) are Enable and WAN Address (hex)/DLCI (decimal). The latter is identical with the same parameter listed for the Adjacent Host Configuration window. The description is repeated here for your convenience.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Sets the state (active or inactive) of the adjacent host record in the IPX routing tables.
Instructions:	Select Disable to make the adjacent host record inactive in the IPX host table. Select Enable to make the adjacent host record active in the IPX host table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.26.1.2

Parameter:	**WAN Address (hex)/DLCI (decimal)**
Default:	None
Options:	WAN Address | Data Link Connection Identifier
Function:	Lets you enter a WAN address or a DLCI. The format depends on the underlying data link protocol type.
Instructions:	Enter a WAN address of up to 16 hexadecimal characters if the interface is on an ATM or SMDS network. Enter a decimal DLCI number if the interface is on a Frame Relay network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.26.1.6

Deleting an Adjacent Host

To delete an adjacent host:

1. **Select from the IPX Adjacent Hosts window (refer to Figure 4-13) the adjacent host you want to delete from the node configuration.**
2. **Click on Delete in the Adjacent Hosts window.**

The system software deletes the Adjacent Host entry you selected, and the entry disappears from the list of adjacent hosts in the Adjacent Hosts window.

Using Static Routes

IPX static routes are user-specified routing table entries. Static routes, like routes learned through RIP, are maintained in the IPX routing table. Unlike routes learned through RIP, however, static routes do not expire. Static routes remain in the IPX routing table until they are reconfigured manually.

The following sections show you how to add, edit, and delete IPX static routes in a Bay Networks router configuration. You perform these functions from the IPX Static Routes window. Begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables**. The IPX Static Interface Tables Configuration window appears (refer to Figure 4-12). Click on Static Route. The IPX Static Routes window appears (Figure 4-15).

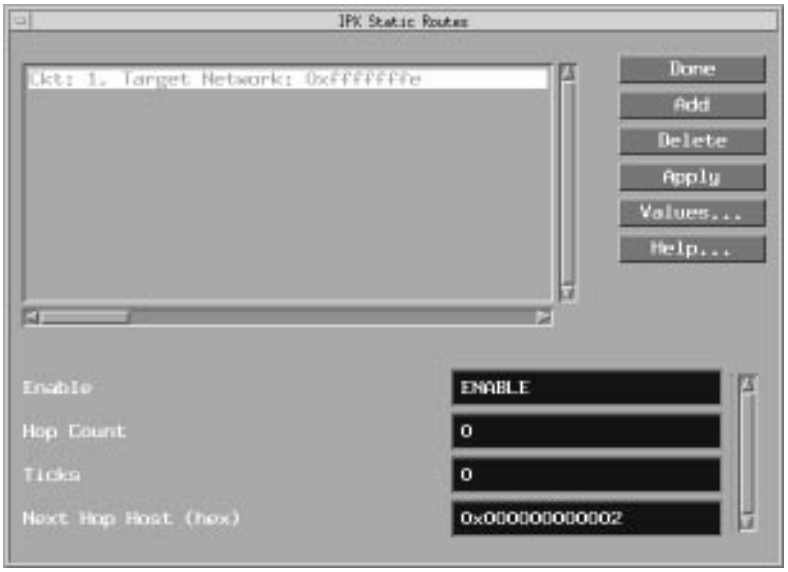

Figure 4-15. IPX Static Routes Window

Refer to the following sections to add, edit, and delete static routes.

Note: *The following rule applies when RIP is disabled on a WAN interface:*

To map an IPX host address to a data link address in a Frame Relay, SMDS, or ATM network, which allows the router to send packets over a static route, you must configure an adjacent host and edit the DLCI parameter in the IPX Adjacent Hosts window before you configure a static route to that adjacent host.

The IPX Static Routes window displays each Static Route entry in the router configuration as follows:

<circuit_index>.<target_network>

Adding a Static Route

To add a static route, begin at the IPX Static Routes window (refer to Figure 4-15) and proceed as follows:

1. **Click on Add.**

   The IPX Static Route Configuration window appears (refer to Figure 4-16).

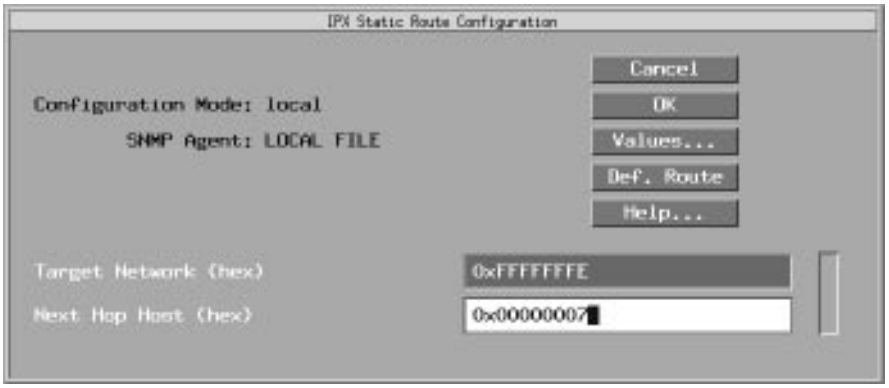

Figure 4-16. IPX Static Route Configuration Window

2. **Edit the parameters, using the parameter descriptions that follow as guidelines.**
3. **Click on OK to save your entries.**

The IPX Static Routes window (refer to Figure 4-15) reappears immediately after you click on OK.

Adding a Default Route

When Default Route is enabled, the router will use a default route if one exists. You can add a default route by clicking Def. Route when you add a static route. This puts the value 0xFFFFFFFE into the Target Network field. You must still specify an explicit value for the next-hop host parameter. When you click on OK, the IPX Static Routes window reappears, and the default route appears in the subwindow, next to the circuit index.

IPX Static Route Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Static Route Configuration window.

Parameter:	**Target Network (hex)**
Default:	None
Range:	Any valid network address in hexadecimal notation
Function:	Specifies the address of the network to which you want to configure the static route.
Instructions:	Enter a network address of up to 8 hexadecimal characters or click on Def. Route to have the Configuration Manager fill in the default route 0xFFFFFFFE.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.19.1.5

Note: *The Configuration Manager does not let you reconfigure the Target Network parameter for a static route. If you want to change this parameter, you must delete the static route and add a new route with the proper information. However, you can reconfigure all other parameters associated with a static route.*

Parameter:	**Next Hop Host (hex)**
Default:	None
Options:	Any valid host address in hexadecimal notation
Function:	Specifies the address of the next-hop host in the static routing path.
Instructions:	Enter a host address of up to 12 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.19.1.8

Editing a Static Route

You can edit the configurable parameters of a static route in the node configuration.

To edit the configurable parameters associated with an existing static route, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. Click on Static Route. The IPX Static Routes window appears (refer to Figure 4-15). From this window, proceed as follows:

1. **Select the static route you want to edit by clicking on the appropriate entry in the list of static routes.**
2. **Click on any parameter value you want to change; then enter a new value.**
3. **Click on Apply to save your changes.**
4. **Click on Done to exit the IPX Static Routes window.**

IPX Static Route Parameter Descriptions

This section describes how to set all parameters shown on the IPX Static Routes window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies the state (active or inactive) of the static route record in the IPX routing tables.
Instructions:	Select Disable to make the static route record inactive in the IPX routing table. Select Enable to make the static route record active in the IPX routing table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.19.1.2

Parameter:	**Hop Count**
Default:	0
Range:	0 to the value of the Maximum Hops parameter, minus 1
Function:	The IPX router uses Hop Count when determining the best route for a datagram to follow. The hop count is also propagated through RIP. The default setting of 0 for static routes means “use the hop count associated with the interface.”
Instructions:	Accept the default (0) or enter a value from 1 to one less than the maximum number of hops.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.19.1.7

Parameter:	**Ticks**
Default:	0
Range:	0 to maximum positive integer
Function:	Specifies the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route. The IPX router uses tick cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes means “use the tick count associated with the interface.”
Instructions:	Accept the default value (0) or enter a value from 1 to the maximum positive integer.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.19.1.6

Parameter:	**Next Hop Host (hex)**
Default:	None
Range:	Any valid host address in hexadecimal notation
Function:	Specifies the address of the next-hop host in the static routing path.
Instructions:	Enter a host address of up to 12 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.19.1.8

Deleting a Static Route

To delete an IPX static route:

1. **Select from the IPX Static Routes window the static route you want to delete from the node configuration.**
2. **Click on Delete in the IPX Static Routes window (refer to Figure 4-15).**

The system software deletes the Static Route entry you selected, and the entry disappears from the list of static routes in the IPX Static Routes window.

Using Static Services

Once you add an IPX interface to a LAN circuit, you can use the Configuration Manager to add, edit, or delete static services on that interface. (For more information on static services, refer to Chapter 1.)

The static service provides an alternative to broadcasting Service Advertisement Protocol (SAP) announcements across a WAN. The static service eliminates WAN traffic (and hence, the use of WAN bandwidth) associated with WAN SAP announcements.

You can add, edit, or delete static services through the IPX Static Services window. To access the window, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. The IPX Static Interface Tables Configuration window appears (refer to Figure 4-12). Click on Static Serv. The IPX Static Services window shown in Figure 4-17 appears:

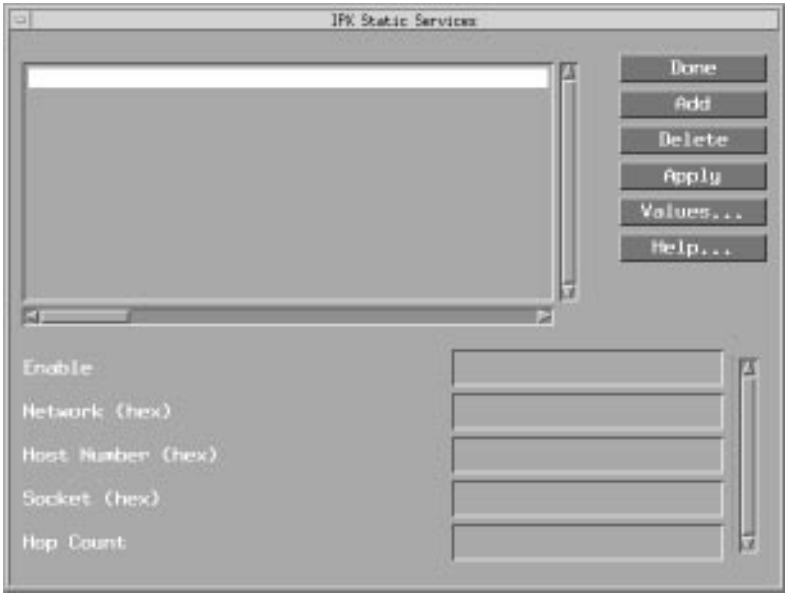

Figure 4-17. IPX Static Services Window

The IPX Static Services window displays each Server entry in the router configuration, as follows:

<circuit_index>, <server_name>, <type_of_service>

Adding a Static Service

To add a static service, begin at the IPX Static Services window (Figure 4-17) and proceed as follows:

1. **Click on Add. The IPX Static Service Configuration window appears (Figure 4-18):**

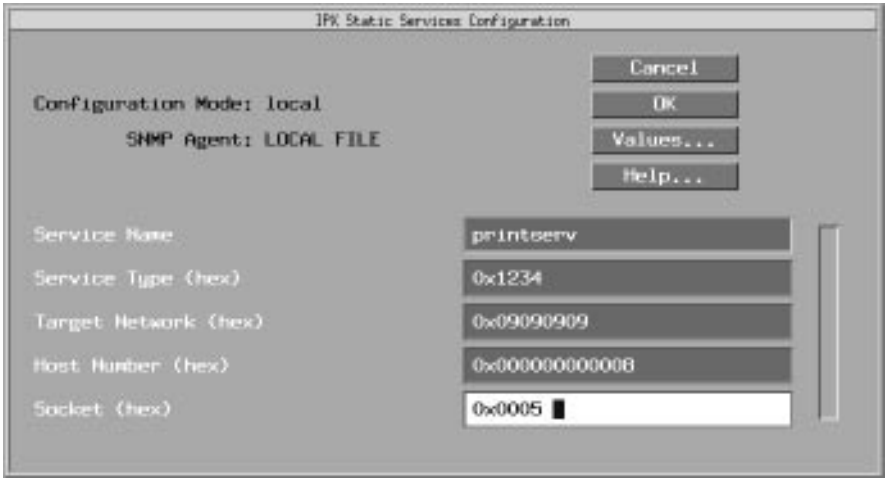

Figure 4-18. IPX Static Service Configuration Window

2. **Edit the parameters, using the parameter descriptions that follow as guidelines.**
3. **Click on OK to save your entries to the configuration file.**

The IPX Static Services window (Figure 4-17) reappears immediately after you click on OK.

IPX Static Service Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Static Service Configuration window.

Parameter:	**Service Name**
Default:	None
Range:	Any valid Novell NetWare server name
Function:	Assigns a symbolic name to the service you want to advertise.
Instructions:	Use the *actual* name of the server that the clients will attach to. It helps if this is a name meaningful to the network administrator. The name must be unique among all names assigned to IPX servers of the same type on the IPX internetwork. See the documentation that came with your NetWare operating system for guidelines on specifying a server name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.5

Parameter:	**Service Type (hex)**
Default:	None
Range:	Any valid Novell server type number in 4-digit hexadecimal format. (The number must be a value between 0x0001 and 0xFFFE, inclusive.)
Function:	Specifies the type of service to advertise from the associated IPX (LAN) interface (for example, 0x0004 for fileserver, 0x0007 for printerserver).
Instructions:	Enter the server type number in 4-digit hexadecimal format. Include leading zeros.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.6

Note: *Refer to Appendix A for a list of common service types (current as of the publication date of this manual).*

Parameter:	**Network (hex)**
Default:	None
Range:	Any valid IPX network address in hexadecimal notation.
Function:	Specifies the network address of this service.
Instructions:	Enter a network address of up to 8 hexadecimal characters. The path to the network you specify for this service must exist as an entry in the IPX routing table. The entry can be learned dynamically by the router, or you can configure the entry as a static route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.7

Parameter:	**Host Number (hex)**
Default:	None
Options:	The address (host ID) of the service.
Function:	Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.
Instructions:	Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server. (For example, most NetWare Server host IDs are usually 0x000000000001.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.8

Parameter:	**Socket (hex)**
Default:	None
Range:	Any valid socket address. (The number must have a value between 0x0001 and 0xFFFE, inclusive.)
Function:	Specifies the socket address of this service.
Instructions:	Enter any valid socket address consisting of up to 4 hexadecimal characters (for example, 0x0451).
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.9

Editing a Static Service

You can customize or edit the configurable parameters of a static service entry for a particular IPX interface.

Note: *The Configuration Manager does not let you change the Service Name or Type parameters you set when you added the static service. To establish new values for these parameters for a particular static service, you must delete that service and configure a new service. You can, however, reconfigure all other parameters associated with a static service.*

To edit the configurable parameters associated with an existing static service, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. Click on Static Serv. The IPX Static Services window appears, as shown in Figure 4-17. From this window, proceed as follows:

1. **Select the static service you want to edit by clicking on the appropriate entry in the list of static services.**
2. **Click on any parameter value you want to change; then enter a new value.**
3. **Click on Apply to save your changes.**
4. **Click on Done to exit the IPX Static Services window.**

IPX Static Service Parameter Descriptions

This section describes how to set all parameters shown on the IPX Static Services window (refer to Figure 4-17).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables a static service previously added to a specific IPX interface.
Instructions:	Select Enable to re-enable a static service previously disabled. This restores client access to NetWare services configured earlier on the IPX interface. Disable a static service to make NetWare services configured earlier unavailable to clients.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.2

Parameter:	**Network (hex)**
Default:	None
Range:	Any valid IPX network address in hexadecimal notation.
Function:	Specifies the network address of this service.
Instructions:	Enter a network address of up to 8 hexadecimal characters. The path to the network you specify for this service must exist as an entry in the IPX routing table. The entry can be learned dynamically by the router, or you can configure the entry as a static route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.7

Parameter:	**Host Number (hex)**
Default:	None
Options:	The address (host ID) of the service.
Function:	Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.
Instructions:	Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.8

Parameter:	**Socket (hex)**
Default:	None
Range:	Any valid socket address. (The number must have a value between 0x0001 and 0xFFFE, inclusive.)
Function:	Specifies the socket address of this service.
Instructions:	Enter any valid socket address consisting of up to 4 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.23.1.9

Parameter:	**Hop Count**
Default:	None
Range:	Any valid number of hops, from 1 to the value of the Maximum Hops parameter, minus 1
Function:	Specifies the number of subsequent router hops required from this router to reach a specific remote Novell server or service.
Instructions:	Enter the number of router hops that exist between the router and the service you want to advertise.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.12.1.10

Deleting a Static Service

To delete a static service:

1. **Select from the IPX Static Services window the static service you want to delete from the node configuration.**
2. **Click on Delete in the IPX Static Services window (refer to Figure 4-17).**

The system software deletes the static service entry you selected, and the entry disappears from the list of static services in the IPX Static Services window.

Using Route Filters

You can shield the view of networks from users on different network segments by configuring route filters. Route filters give you greater control over the routing of IPX packets from one area of an IPX internetwork to another. This helps maximize the use of the available bandwidth throughout the IPX internetwork, and helps improve network security by shielding a user's view of other networks.

You can configure inbound or outbound route filters on a per-interface basis, instructing the interface to advertise/accept or drop filtered RIP packets. The action parameter that you define for the filter determines whether the router advertises, accepts, or suppresses RIP packets from routers that match the filter pattern.

IPX route filters uses the network number field in the IPX RIP packet. Network filtering is based on a two-part definition: filter ID and a corresponding mask. A route filter can be inbound, outbound, or both. You can define filters by network address, or by a range of network addresses.

The filter ID and the mask definition work together to determine which addresses are filtered on the interface. The character F in the mask definition requires an exact match with the corresponding character in the filter ID. The mask character 0 matches any hexadecimal character. You can combine the F and 0 characters in any order in the mask to filter any combination of network and/or area addressing schemes used within the IPX internetwork.

For example, suppose you want to filter the range of network addresses from ABCD1200 to ABCD12FF. To do this, you would define:

- A filter ID of ABCD12FF, *and*
- A mask of FFFFFF00

In this example, the filter ID says "This is the pattern to match." The mask says, "The first six characters of the address must match the filter ID, but the last two characters are irrelevant."

You can add, edit, and delete route filters through the IPX Route Filters window. To access this window, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols➔IPX➔Static/Filter Tables** option. The IPX Static Interface Tables Configuration window appears (refer to Figure 4-12). Select the interface you want to change on the subwindow, and click on Route Filter. The IPX Route Filters window appears (Figure 4-19).

Figure 4-19. IPX Route Filters Window (Top)

You have to scroll the list of parameters to see all the fields. Figure 4-20 shows the bottom of the IPX Route Filters window.

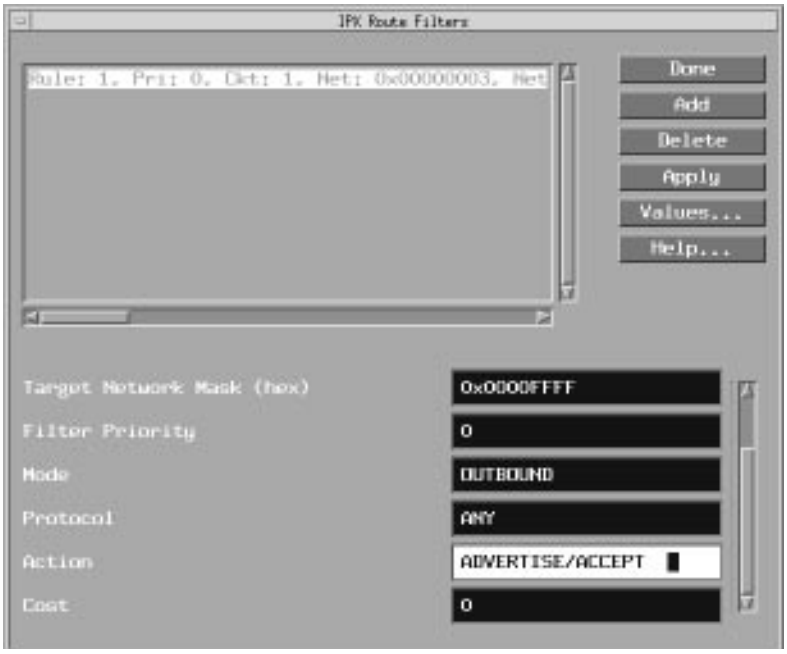

Figure 4-20. IPX Route Filters Window (Bottom)

The IPX Route Filters window displays each route filter entry in the router configuration, as follows:

<rule_number>, <priority>, <circuit_index>, <filter_ID>, <filter_mask>

Once you have configured route filters, you can easily drop all routes to allow one or more specific routes. To drop all routes, apply a filter at a low priority. For example, in the IPX Route Filters window, enter the value 0xFFFFFFFF for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask, and set the Action parameter to Suppress.

Add the filters you want by specifying higher priorities to advertise specific routes.For example, enter the value 0x3081be86 for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask parameter, and set the Priority parameter to 1.

Adding a Route Filter

To add a route filter, begin at the IPX Route Filters window (Figure 4-19), and proceed as follows:

1. **Click on Add. The IPX Route Filter Configuration window appears (Figure 4-21).**

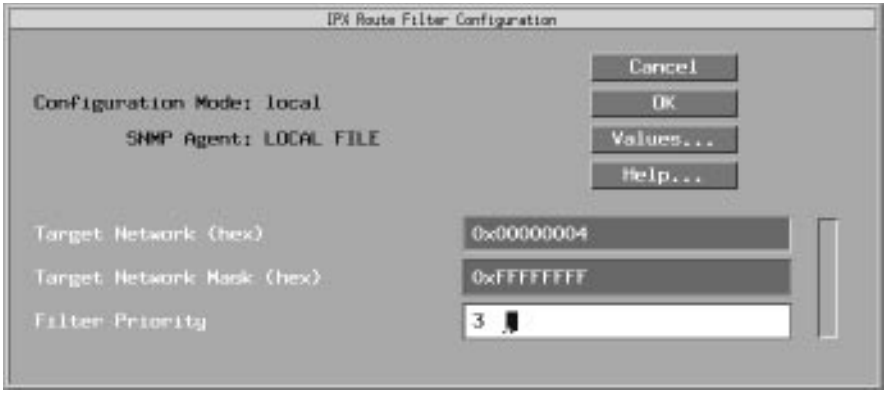

Figure 4-21. IPX Route Filter Configuration Window

2. **Enter the target network for which you want to filter RIP packets.**
3. **Enter the mask that you want to apply.**
4. **Enter the filter priority.**
5. **Click on OK to save your entry and exit the window.**

Editing Route Filter Configuration Parameters

This section describes all parameters shown in the IPX Route Filter Configuration window.

Parameter:	**Target Network**
Default:	None
Range:	Any valid NetWare address in hexadecimal format
Function:	Identifies the network on which you want to apply the filter (the "filter ID" in the previous example).
Instructions:	Enter the address of the target network in hexadecimal format. Using a mask, you can make this stand for a single ID or for a range of IDs with similar addresses. You can select all IDs by entering the wildcard value 0xFFFFFFF.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.6

Parameter:	**Target Network Mask**
Default:	None
Options:	0x00000000 to 0xFFFFFFFF
Function:	Specifies the mask that you want to apply.
Instructions:	Enter 8 hexadecimal characters. The character F in the mask definition requires an exact match with the corresponding character in the filter ID. The mask character 0 matches any alphanumeric character. You can combine the F and 0 characters in any order in the mask to filter any combination of network addressing schemes used within the IPX internetwork.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.7

Parameter:	**Filter Priority**
Default:	None
Options:	0 to the maximum positive integer
Function:	Specifies the priority of this filter in relation to other filters of the same type.
Instructions:	You set the filter's priority with this parameter. Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.13

Editing an IPX Route Filter

You can edit the configurable parameters of a route filter in the node configuration. To edit the configurable parameters associated with an existing route filter, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. The IPX Static Interface Tables Configuration window appears (refer to Figure 4-12). Click on Route Filter. The IPX Route Filters window appears, as shown in Figure 4-19. From this window, proceed as follows:

1. **Select the route filter that you want to edit by clicking on the appropriate entry in the list of route filters.**
2. **Click on any parameter value you want to change; then enter a new value.**
3. **Click on Apply to save your changes.**
4. **Click on Done to exit the IPX Route Filters window.**

IPX Route Filter Parameter Descriptions

This section describes how to set all the parameters shown on the IPX Route Filters window (Figure 4-19).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables a route filter previously added to a specific IPX interface.
Instructions:	Select Enable to enable a route filter.
	Select Disable to disable a route filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.2

Parameter:	**Target Network**
Default:	None
Range:	Any valid NetWare address in hexadecimal format
Function:	Identifies the network on which you want to apply the filter (that is, the “filter ID” in the previous example).
Instructions:	Enter the address of the target network in hexadecimal format. Using a filter, you can make this stand for a single ID or for a range of IDs with similar addresses. You can select all IDs by entering the wildcard value 0xFFFFFFF.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.6

Parameter:	**Target Network Mask**
Default:	None
Options:	0x00000000 to 0xFFFFFFFF
Function:	Specifies the mask that you want to apply.
Instructions:	Enter 8 hexadecimal characters. The character F in the mask definition requires an exact match with the corresponding character in the filter ID. The mask character 0 matches any alphanumeric character. You can combine the F and 0 characters in any order in the mask to filter any combination of network addressing schemes used within the IPX internetwork.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.7

Parameter:	**Filter Priority**
Default:	None
Options:	0 to the maximum positive integer
Function:	Specifies the priority of this filter in relation to other filters of the same type.
Instructions:	You set the filter's priority with this parameter. Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.13

Parameter:	**Mode**
Default:	Outbound
Options:	Outbound | Inbound | Both
Function:	Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.
Instructions:	Accept the default, Outbound, if you want to apply the filter to RIP packets advertised by the specified interface. Specify Inbound if you want to apply the filter to RIP packets coming into this interface. Specify Both if you want to filter both inbound and outbound packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.8

Parameter:	**Protocol**
Default:	Any
Options:	Any | Local | RIP | Static
Function:	Applies this filter only to routes learned on the specified protocol when sending RIP updates. This does not apply to Inbound routes.
Instructions:	Specify the protocol on which you want to apply the filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.10

Parameter:	**Action**
Default:	Advertise/Accept
Options:	Advertise/Accept | Suppress
Function:	Specifies how to process any RIP advertisement that matches the route filter criteria you established.
Instructions:	Select Advertise/Accept to enable the filter to allow advertisement or acceptance of routes that match the specified route filter criteria. Select Suppress to configure the IPX router to drop RIP advertisements that match the specified route filter criteria.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.9

Parameter:	**Cost**
Default:	1 (for hop- or tick-based routing)
Options:	1 to maximum positive integer (if tick-based routing is enabled) 1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)
Function:	Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent RIP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user. Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router. If the filter is an *inbound* filter, the entered cost replaces the cost associated with the route in the RIP advertisement, and the router uses this cost in its calculations. If this is an *outbound* filter, the entered cost replaces the route's cost that this router advertises in RIP packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.11

Deleting an IPX Route Filter

To delete an IPX route filter, begin at the IPX Route Filters window (refer to Figure 4-19) and do the following.

1. **Select from the IPX Route Filters window the route filter that you want to delete from the node configuration.**
2. **Click on Delete. The system software deletes the route filter you selected, and the entry disappears from the list of route filters in the IPX Route Filters window.**

Using SAP Filters

Chapter 1 describes how and why to filter SAP packets. Briefly, a filter is a pattern for matching a service name or service network. The router scans incoming and outgoing SAP packets to see whether certain fields in the packet match the filter. (The type of filter — service name or service network — determines which fields the router examines.) When you set up the filter, you can specify what the router does with the services in the packet when it finds a match.

You can create SAP filters on Bay Networks routers in your network to regulate both incoming and outgoing SAP advertisements. You can use SAP filters to control the size of resident SAP services tables and reduce bandwidth waste on your network due to SAP broadcast overhead. You can also create SAP filters to limit a user's view of services located elsewhere on the network.

Each SAP filter consists of a service name or network number, a service type, a priority, and a configurable action parameter. (You can also include wildcards or patterns to be matched). As a result, you can tailor SAP filters to your site requirements, improving network security by controlling access and preserving bandwidth by limiting the SAP packet traffic. On a given interface, you can configure a filter as inbound, outbound, or both.

The following sections describe how to construct SAP filters, then how to configure them on an interface.

Using Wildcards and Pattern Matching with SAP Filters

Wildcards and pattern matching are short-cut techniques for setting up SAP filters. Wildcards are characters that match zero or more instances of any valid character. In other words, a wildcard in a filter matches any allowable character(s), depending on which wildcard you specify. Pattern matching lets you selectively filter by named entities. The following sections describe each of these techniques.

Using Wildcards with SAP Filters

Wildcards in SAP filters let you configure a single SAP filter to match a set of services. When you use wildcards, you can configure the filter based on the service name, which lets you configure a SAP filter based on the characters represented in the service name field of an IPX SAP packet. The service name field contains the 48-byte character string name that is assigned to a NetWare server. The service name, in combination with the service type, uniquely identifies a service on the internetwork. You can use a wildcard SAP filter configured using the service name field to shield users' view of services that reside on a group of servers that use a common naming convention.

The wildcard characters are

* (Asterisk) matches any number of instances (zero or more) of the previous character.

• (Period or dot) matches any *single* character.

For example, suppose an organization has ten servers within its network, each providing a variety of different services. Five of the servers have names that begin with the character **p**, while the other servers have names that start with a different character. You could then define a single SAP filter **p•*** that would filter all SAP information for all five servers whose server name begins with the character **p**.

Similarly, a SAP filter defined as p•int would match the server names **print**, **point**, and **paint**, but not the server name **poing**, because the wildcard character • matches only a single character in the same position in the string that makes up the server name.

Using Pattern Matching with SAP Filters

You can also filter SAP packets by, matching a filter pattern that you define as a *regular expression*, using the characters shown in Table 4-1. The software compares this regular expression against a service name and returns an indication of whether it finds a match. Functionally, pattern matching on SAP filters is similar to the UNIX **grep** command.

Table 4-1. Characters in SAP Pattern Matching Filters

Filter Character	Function
C	Matches any character, except those listed below. An ordinary character (like a, b, 7, or q) matches only itself.
\ (Backslash)	The backslash (/) is the escape character. Use this to match a character that would otherwise have special meaning to the software. The special characters that must be preceded by a backslash to match themselves are **** (backslash) **.** (period or dot) **[** (left bracket) **?** (question mark) ***** (asterisk) **{** (left brace) **(** (left parenthesis) **)** (right parenthesis) **|** (vertical bar) **$** (currency symbol) must be quoted only when it's the last character to be matched. Any other quoted character following a backslash matches itself. For example, to match a backslash (\) in a string, include the following in the filter expression: \\
. (Dot or period)	Matches a single character
[c...]	As the rightmost element in a string, this element tells the filter to match *any one* of the characters enclosed in the brackets. To use a right bracket (]) as one of the characters to be matched, make it the first character in the string. The expression: [ ]abc] matches any of the characters], a, b, or c

Table 4-1. Characters in SAP Pattern Matching Filters *(continued)*

Filter Character	Function
[^c...]	When a caret is the first character of the enclosed string, the filter expression matches any character *except* those in the remainder of the string. For example, the expression [^45678] matches any character except 4, 5, 6, 7, or 8. To include a right bracket (]) in the string of filtered characters, place it directly after the caret. For example, the expression [^] abc] matches every character except], a, b, or c.
[l-r]	The minus sign between two characters indicates a range of consecutive ASCII characters to match. This bracketed string of characters is known as a *character class*. For example, the range [0-9] is equivalent to the string: [0123456789] The minus sign (-) is treated as an ordinary character if it occurs first (or first after an initial ^ character) or last in a string.

You can also construct longer filters by combining (that is, concatenating) these single-character regular expressions using the rules and operators listed in Table 4-2. A filter made up of a concatenation of regular expressions matches a concatenation of text strings, each of which is a match for a successive regular expression in the search pattern.

Table 4-2. Concatenation Rules and Operators

Rule/Operator	Interpretation
? (Question Mark)	A single-character regular expression followed by a question mark (?) matches *zero or exactly one* occurrence of that single-character regular expression. For example, [a-z]**?** matches any string of either zero lowercase letters or exactly one lowercase letter.
***** (Asterisk)	A single character regular expression followed by an asterisk (*) matches zero or more occurrences of that single-character regular expression. For example, [a-z]***** matches any string of zero or more lowercase letters.
+ (Plus Sign)	A single-character regular expression followed by a plus sign (+) matches one or more occurrences of that single-character regular expression. For example, [a-z]+ matches any string with one or more lowercase letters.

Table 4-2. Concatenation Rules and Operators *(continued)*

Rule/Operator	Interpretation
{m} **{m,}** **{m,n}** (where m and n are integers)	A one-character regular expression followed by {m}, {m,}, or {m,n} is a regular expression that matches a range of occurrences of the one-character regular expression. The values m and n must be non-negative integers less than 255. The symbols in braces mean the following: {m} matches *exactly* m occurrences {m,} matches *at least* m occurrences {m,n} matches *any number* of occurrences between m and n. Whenever a choice exists, the regular expression matches as many occurrences as possible. For example, the **?** operator is equivalent to {0,1}, the ***** operator is equivalent to {0,}, and the **+** operator is equivalent to {1,}.
Use the following operators to construct regular expressions from more-than-single-character regular expressions.	
(...) (Regular expression(s) enclosed in parentheses)	A regular expression enclosed within parentheses matches whatever the unadorned regular expression matches. You use parentheses to group a series of regular expressions that you want to have treated as a single-character regular expression. For example, the regular expression **0[Xx]?** matches a 0 that may or may not be followed by one X or x, while the regular expression **(0[Xx])?** matches either nothing or the string “0X” or the string “0x”. You can have up to nine such substrings in a regular expression, and you can nest parentheses.
| (Vertical bar)	Two regular expressions separated by the vertical bar (|) match either a match for the first or a match for the second. These two regular expressions are the longest that can be created subject to parentheses grouping. For example, these regular expressions are grouped as follows: and|or = and | or and*|o+r = and* | o+r a(nd|o)r = a, plus either nd or o, plus r

The server name filters take precedence over the service network filters. Both service name and service network filters have an associated priority, with smaller values denoting a higher priority. Matching is performed by first checking all service name filters in order by priority. If a match isn’t found, then the service network filters are checked in order by priority.

For example, you may want to advertise from an IPX interface only one type of service (Type 4) belonging to a particular server (Server 1). You can configure:

- A service name SAP filter with a target service name of Server 1, a service type of 4, and an action to advertise.
- A service network filter with a target network of 0xFFFFFFFF, a type of 0xFFFF, and an action to suppress. (This service network filter prevents all other services from being advertised from the interface.)

Using similar specifications and an action to suppress, you could exclude from an IPX interface a type of service from a particular server.

Note: *The order in which you create SAP filters does not affect filter precedence.*

An Example of Using SAP Filters

The following example describes a situation in which you might want to configure SAP filters. An office complex contains three buildings. The people in each building use only the print services within their own building and have no need to send files to printers outside their building. To free up wasted bandwidth, you could configure a SAP filter that suppresses print server advertisements on the interfaces of the routers that connect the three buildings.

To suppress print server advertisements, configure a service network filter on the interfaces of the routers that connect the three buildings and suppress the advertisement of Server Type 0x0047 (print server) for all networks (0xFFFFFFFF). Refer to Appendix A for a list of common server types.

Configuring Service Network Filters

Service network filters let you reduce IPX SAP network traffic, depending on the way you configure the filters.

You can add, edit, and delete service network filters for each interface through the IPX Service Network Filters window. To access this window, begin at the Configuration Manager window (refer to Figure 4-1) and select the option **Protocols→IPX→Static/Filter Tables**. The IPX Static Interface Tables Configuration window appears (refer to Figure 4-12).

Then select the interface on which you want to add or change the filter from the subwindow and click on Net Filter. The IPX Service Network Filters window appears. Figure 4-22 shows the top of this window.

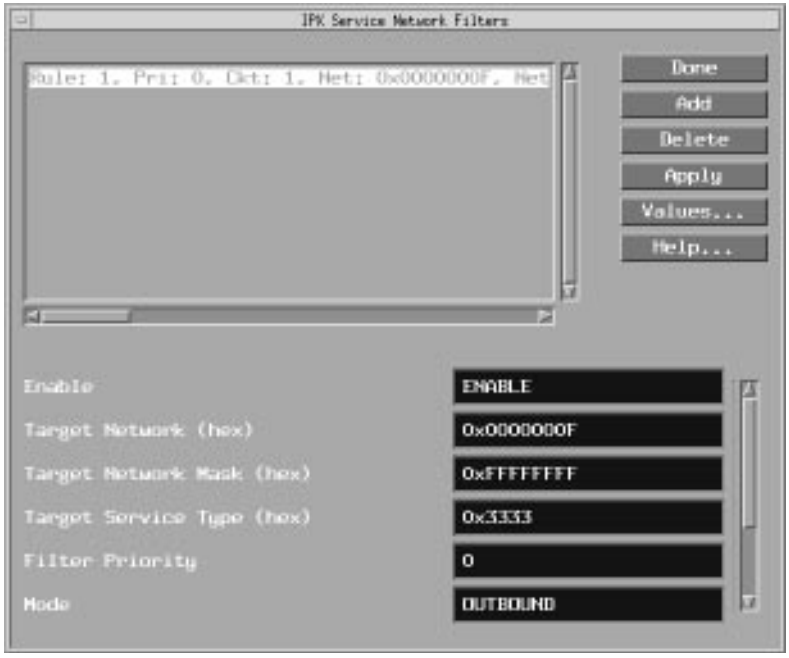

Figure 4-22. IPX Service Network Filters Window (Top)

You have to scroll the window to see all the parameters. Figure 4-23 shows the bottom of this window.

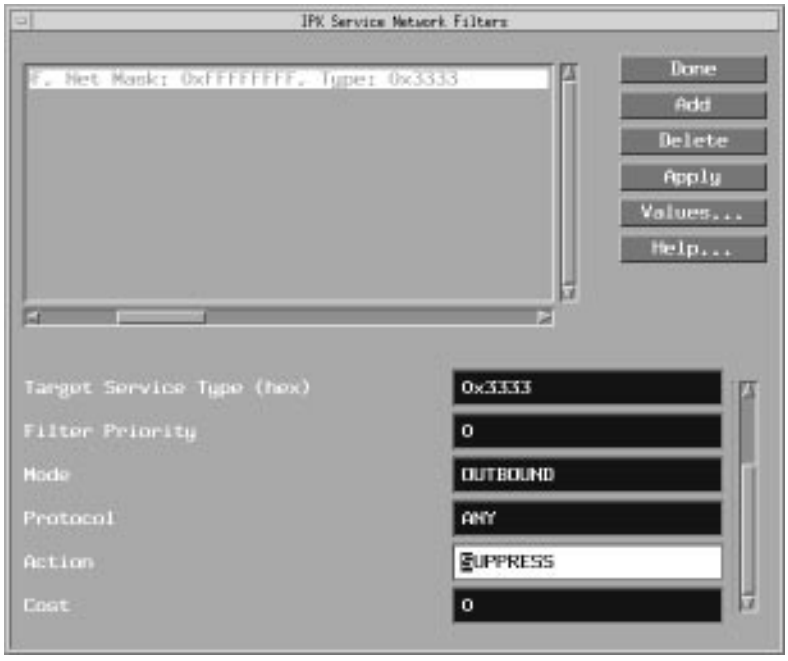

Figure 4-23. IPX Service Network Filters Window (Bottom)

The IPX Service Network window displays each service network filter entry in the router configuration, as follows:

<filter/rule_no.>, <filter_priority>, <circuit_number>, <target_network_number>, <target_network_mask>, <target_service_type>

Once you have configured SAP filters, you can easily drop all services to allow one or more specific services. To drop all services, apply a filter at a low priority. For example, in the IPX Service Network Filters window, enter the value 0xFFFFFFFF for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask, and set the Action parameter to Suppress.

Add the filters you want by specifying higher priorities to advertise specific services.For example, enter the value 0x3081be86 for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask parameter, the value 0x0004 for the Target Service Type parameter, and set the Priority parameter to 1.

Adding a Service Network Filter

To add a service network filter, begin at the IPX Service Network Filters window (refer to Figure 4-22) and proceed as follows:

1. **Click on Add.**

   The IPX Service Network Filter Configuration window appears (Figure 4-24).

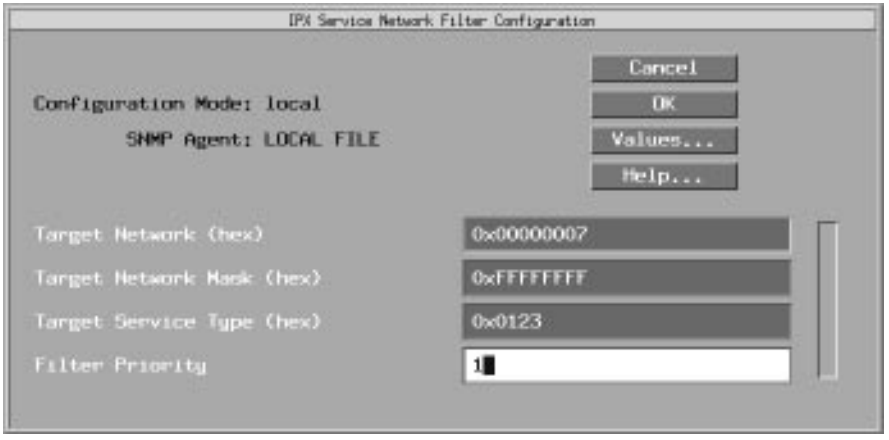

Figure 4-24. IPX Service Network Filter Configuration Window

2. **Enter the network address of a service that the service network filter should recognize.**
3. **Enter the mask that you want to apply to that network address.**
4. **Enter the type of network service that the service network filter should recognize.**
5. **Enter the filter priority.**
6. **Click on OK to save your entry and exit the window.**

   The IPX Service Network Filters window reappears immediately after you click on OK.

Service Network Filter Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Service Network Filter Configuration window.

Parameter:	**Target Network (hex)**
Default:	None
Range:	Any valid network address in hexadecimal notation.
Function:	Specifies the network that you want to filter. The value 0xFFFFFFFF specifies all networks.
Instructions:	Enter a network address of up to 8 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.6

Parameter:	**Target Network Mask (hex)**
Default:	None
Range:	Any valid IPX network address in hexadecimal notation
Function:	The mask, combined with the Target Network parameter value, determines which networks will be filtered.
Instructions:	Enter a network address or filter pattern of up to 8 hexadecimal characters. A mask of 0xFFFFFFFF specifies an exact match with the network address specified in the Target Network parameter. You can specify all networks by entering a Target Network of 0xFFFFFFFF and a Target Network Mask of 0xFFFFFFFF.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.7

Parameter:	**Target Service Type (hex)**
Default:	None
Range:	Any valid Novell server type number in 4-digit hexadecimal format
Function:	Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of 0xFFFF. See Appendix A for a list of valid server types.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.8

Parameter:	**Filter Priority**
Default:	None
Options:	0 to the maximum positive integer
Function:	Specifies the priority of this filter in relation to other filters of the same type.
Instructions:	Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.14

Editing a Service Network Filter

You can customize or edit the configurable parameters of a service network filter for a particular IPX interface.

To edit the configurable parameters associated with an existing network-level SAP filter, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. Select the interface on which you want to apply the filter. Click on Net Filter. The IPX Service Network Filters window appears, as shown in Figure 4-22. From this window, proceed as follows:

1. **Select the filter you want to edit by clicking on the appropriate entry in the list of service network filters.**
2. **Click on any parameter value you want to change; then enter a new value.**
3. **Click on Apply to save your changes.**
4. **Click on Done to exit the IPX Service Network Filters window.**

IPX Service Network Filter Parameter Descriptions

This section describes all parameters shown in the IPX Service Network Filters window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the service network filter displayed is active on this interface.
Instructions:	Select Enable to enable the service network filter. Select Disable to disable the service network filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.2

Parameter:	**Target Network (hex)**
Default:	None
Range:	Any valid NetWare address in hexadecimal notation
Function:	Specifies the network on which you want to apply the service network filter.
Instructions:	Enter the address of the target network in hexadecimal format. Using a mask, you can make this stand for a single network or a range of networks with similar addresses. You can specify all networks by entering a Target Network of 0xFFFFFFF and a Target Network Mask of 0xFFFFFFF.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.6

Parameter:	**Target Network Mask (hex)**
Default:	None
Range:	Any valid IPX network address in hexadecimal notation
Function:	The mask, combined with the Target Network parameter value, determines which networks will be filtered.
Instructions:	Enter a network address or filter pattern of up to 8 hexadecimal characters. A mask of 0xFFFFFFFF specifies an exact match with the network address specified in the Target Network parameter. You can specify all networks by entering a Target Network of 0xFFFFFFFF and a Target Network Mask of 0xFFFFFFFF. A value of 0x0 is invalid.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.7

Parameter:	**Target Service Type (hex)**
Default:	None
Range:	Any valid Novell server type number in 4-digit hexadecimal format
Function:	Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter the server type number in 4-digit hexadecimal format. Include leading zeros. For all types, enter a value of 0xFFFF. See Appendix A for a list of valid server types.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.8

Parameter:	**Filter Priority**
Default:	None
Options:	0 to the maximum positive integer
Function:	Specifies the priority of this filter in relation to other filters of the same type.
Instructions:	Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.14

Parameter:	**Mode**
Default:	Outbound
Options:	Outbound | Inbound | Both
Function:	Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.
Instructions:	Accept the default, Outbound, if you want to apply the filter to SAP packets advertised by the specified interface. Specify Inbound if you want to apply the filter to SAP packets coming into this interface. Specify Both if you want to filter both inbound and outbound packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.9

Parameter:	**Protocol**
Default:	Any
Options:	Any | Local | Static | SAP
Function:	Applies this outbound filter only to services learned on the specified protocol when sending SAP updates. This does not apply to inbound services.
Instructions:	Specify the protocol on which you want to apply the filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.11

Parameter:	**Action**
Default:	Advertise/Accept
Options:	Advertise/Accept | Suppress
Function:	Specifies how to process any SAP advertisement that matches the SAP filter criteria you established in the Target Network and Target Service Type parameters.
Instructions:	Select Advertise/Accept to enable the filter to allow advertisement or acceptance of services that match the filter criteria you established in the Target Network and Target Service Type parameters. Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Target Network and Target Service Type parameters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.10

Parameter:	**Cost**
Default:	1 (for hop- or tick-based routing)
Range:	1 to maximum positive integer (if tick-based routing is enabled) 1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)
Function:	Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent SAP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router. If the filter is an *inbound* filter, the entered cost replaces the cost associated with the server in SAP advertisements sent from this router. If this is an *outbound* filter, the entered cost replaces the server's cost that is advertised in SAP packets by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.12

Deleting a Service Network Filter

To delete a SAP network-level filter:

1. **Select from the IPX Service Network Filters window the filter you want to delete from the node configuration.**
2. **Click on Delete in the IPX Service Network Filters window (refer to Figure 4-22).**

The system software deletes the filter entry you selected, and the entry disappears from the list of SAP network-level filters in the IPX Service Network window.

Editing Service Name Filter Parameters

The service name filters function lets you reduce network traffic by configuring service name filters.

You can add, edit, and delete service name filters through the IPX Service Name Filters window. To access this window, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. The IPX Static Interface Tables Configuration window appears (refer to Figure 4-12). Click on Name Filter. The IPX Service Name Filters window appears (Figure 4-25 and Figure 4-26).

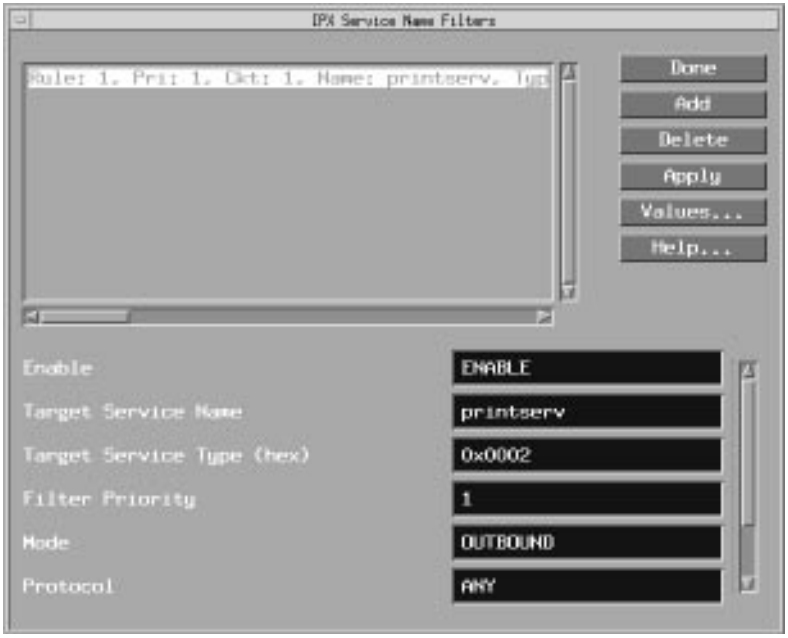

Figure 4-25. IPX Service Name Filters Window (Top)

This is a scrollable window. You have to scroll to see the rest of the parameter fields. Figure 4-26 shows the bottom of the IPX Server Name Filters window.

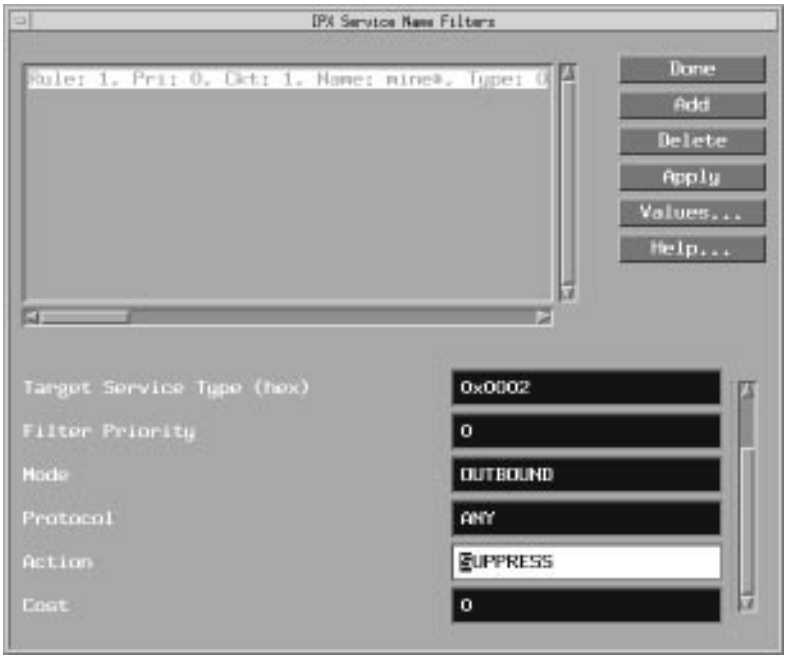

Figure 4-26. IPX Service Name Filters Window (Bottom)

The IPX Service Name Filters window displays each service name filter entry in the router configuration as follows:

<filter/rule_no.>, <filter_priority>, <circuit_index>, <target_service_name>, <target_service_type>

Adding a Service Name Filter

To add a service name filter, begin at the IPX Service Name Filters window (refer to Figure 4-25) and proceed as follows:

1. **Click on Add.**

   The IPX Service Name Filter Configuration window appears (Figure 4-27).

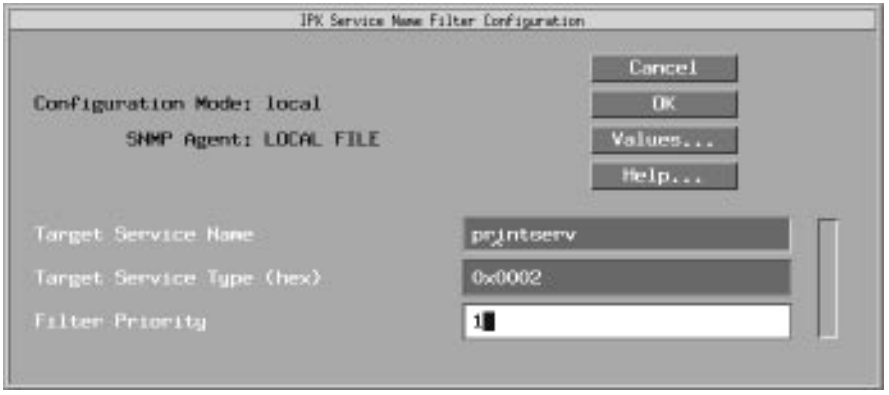

Figure 4-27. IPX Service Name Filter Configuration Window

2. **Enter the name of the service (Target Service Name) that the service name filter should recognize.**
3. **Enter the type of service that the service name filter should recognize.**

   (The filter should allow any frames that contain the target server name and service type information you specified in Steps 2 and 3 onto the segment associated with the interface.)
4. **Click on OK to save your entry and exit the IPX Service Name Configuration window.**

IPX Service Name Filter Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Service Name Filter Configuration window.

Parameter:	**Target Service Name**
Default:	None
Range:	Any valid alphanumeric server name or one containing wildcard characters or a pattern-matching regular expression
Function:	This is the filter that you want to apply. It can specify the name of the server to which you are applying the service name filter, or it can be a filter containing a wildcard or a pattern (regular expression) to be matched. (See “Using Wildcards with SAP Filters” and “Using Pattern Matching with SAP Filters” for lists of these characters.)
Instructions:	Enter a service name or filter pattern consisting of up to 48 alphanumeric characters, optionally including wildcards or a regular expression (pattern).
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.6

Parameter:	**Target Service Type (hex)**
Default:	None
Range:	Any valid Novell service type number in 4-digit hexadecimal format
Function:	Specifies the type of service that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter the service type number in 4-digit hexadecimal format. Include leading zeros. For all types, enter a value of FFFF. See Appendix A for a list of valid service types.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.7

Parameter:	**Filter Priority**
Default:	None
Range:	0 to the maximum positive integer
Function:	Specifies the priority of this filter in relation to other filters of the same type.
Instructions:	Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.13

Editing a Service Name Filter

You can edit the configurable parameters of a service name filter entry in the node configuration.

To edit the configurable parameters associated with an existing service name filter, begin at the Configuration Manager window (refer to Figure 4-1) and select the **Protocols→IPX→Static/Filter Tables** option. Click on Name Filter. The IPX Service Name Filters window appears (refer to Figure 4-25). From this window, proceed as follows:

1. **Select the filter you want to edit by clicking on the appropriate entry in the list of filters.**
2. **Click on any parameter value you want to change, then enter a new value.**
3. **Click on Apply to save your changes.**
4. **Click on Done to exit the IPX Service Name Filters window.**

IPX Service Name Filter Parameter Descriptions

This section describes how to set all parameters shown on the IPX Service Name Filters window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the service name filter displayed is active on this interface.
Instructions:	Select Enable to enable the service name filter. Select Disable to disable the service name filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.2

Parameter:	**Target Service Name**
Default:	None
Range:	Any valid alphanumeric server name or one containing wildcard characters or a pattern-matching regular expression. (See “Using Wildcards with SAP Filters” and “Using Pattern Matching with SAP Filters” for lists of these characters.)
Function:	This is the filter that you want to apply. It can specify the name of the server to which you are applying the server-level SAP filter, or it can be a filter containing a wildcard or a pattern (regular expression) to be matched.
Instructions:	Enter a service name or filter pattern consisting of up to 48 alphanumeric characters, optionally including wildcards or a regular expression (pattern).
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.6

Parameter:	**Target Service Type (hex)**
Default:	None
Range:	Any valid Novell server type number in 4-digit hexadecimal format
Function:	Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of 0xFFFF. See Appendix A for a list of valid service types.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.7

Parameter:	**Filter Priority**
Default:	None
Range:	0 to the maximum positive integer
Function:	Specifies the priority of this filter in relation to other filters of the same type.
Instructions:	Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.13

Parameter:	**Mode**
Default:	Outbound
Options:	Outbound | Inbound | Both
Function:	Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.
Instructions:	Accept the default, Outbound, if you want to apply the filter to SAP packets advertised by the specified interface. Specify Inbound if you want to apply the filter to SAP packets coming into this interface. Specify Both if you want to filter both inbound and outbound packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.8

Parameter:	**Protocol**
Default:	Any
Options:	Any | Local | Static | SAP
Function:	Applies this outbound filter only to services learned on the specified protocol when sending SAP updates. This does not apply to inbound services.
Instructions:	Specify the protocol on which you want to apply the filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.10

Parameter:	**Action**
Default:	Advertise/Accept
Options:	Advertise/Accept | Suppress
Function:	Specifies how to process any SAP advertisement that matches the SAP filter criteria you established in the Target Service Name and Target Service Type parameters.
Instructions:	Select Advertise/Accept to enable the filter to allow advertisement or acceptance of services that match the filter criteria you established in the Service Name and Service Type parameters. Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Service Name and Service Type parameters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.9

Parameter:	**Cost**
Default:	1 (for hop- or tick-based routing)
Range:	1 to maximum positive integer (if tick-based routing is enabled) 1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)
Function:	Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent SAP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router. If the filter is an *inbound* filter, the entered cost replaces the cost associated with the server in the SAP advertisement, and the router uses this cost in its calculations. If this is an *outbound* filter, the entered cost replaces the server's cost that is advertised in SAP packets by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.11

Deleting a Service Name Filter

To delete a service name filter:

1. **Select from the IPX Service Name Filters window (Figure 4-25) the filter you want to delete from the node configuration.**
2. **Click on Delete in the IPX Service Name Filters window.**

The system software deletes the filter entry you selected, and the entry disappears from the list of service name filters in the IPX Service Name Filters window.

Deleting IPX from the Router

To delete IPX from the router, begin at the Configuration Manager window (refer to Figure 4-1) and complete the following steps:

1. **Select the Protocols→IPX→Delete IPX option.**

   A confirmation window appears.

2. **Select OK.**

   The Configuration Manager window appears.

IPX is no longer configured on the router.

Note: *If you delete IPX, the connectors for those interfaces on which IPX was the only protocol enabled are no longer highlighted in the Configuration Manager window. Interfaces must be reconfigured for these connectors; see* Configuring Routers *for instructions.*

Appendix A
Common Service Types and Identifiers

Table A-1. Service Types and Identifiers

Service Type	Hexadecimal Identifier
Wildcard	FFFF
Unknown	0000
User	0001
User Group	0002
Print Queue	0003
NetWare File Server V3.*x*	0004
Job Server	0005
Gateway	0006
Print Server	0007
Archive Queue	0008
Archive Server	0009
Job Queue	000A
Administration	000B
Diagnostics	0017
NetBIOS	0020
NAS SNA Gateway	0021
NACS	0023

Table A-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Remote Bridge Server	0024
Bridge Server	0026
TCP/IP Gateway (Racal-Datacom)	0027
Eicon X.25 Point-to-Point GW	0028
Eicon 3270 Gateway	0029
(CHI) Corp	002A
Unknown	002C
Time Synchronization Server	002D
Archive Srvr Dynamic SAP/SMS TSA	002E
DI3270 Gateway	0045
Advertising Print Server	0047
TCP/IP Gateway (Racal-Datacom)	0048
Unknown	004A
Btrieve VAP 5.*x*	004B
NetWare SQL VAP/NLM	004C
Xtree Network Version	004D
Btrieve VAP 4.*x*	0050
QuickLink (Cubix)	0052
Print Queue User	0053
ARCserve VAP	0055
Eicon X.25 Multi-Point Gateway	0058
ARCserv	0064
ARCserve 3.0	0066
WANcopy Utility	0072
Cheyenne ARCserv 5.0 Intel	0077

Table A-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
TES-NetWare for VMS	007A
Emerald Backup/WATCOM Debugger	0092
TES-NetWare for VMS	0095
NetWare Access Server (NAS)	0098
SQL Server (Named Pipes)	009A
NetWare Access Server	009B
Portable NetWare/SunLink NVT	009E
Progress Database Server	009F
PowerChute APC UPS NLM	00A1
Compaq IDA Status Monitor	00AC
Unknown	0100
Intel LAN Protect Bindery	0102
Oracle Database Server	0103
NetWare 386, Remote Console	0107
Novell SNA Gateway	010F
HP Print Server	0112
CSA MUX	0114
CSA LCA	0115
CSA CM	0116
CSA SMA	0117
CSA DBA	0118
CSA NMA	0119
CSA SSA	011A
CSA STATUS	011B
CSA APPC	011E

Table A-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
SNA TEST (SAA profile)	0126
CSA TRACE	012A
Unknown	012E
Communications Executive	0130
NFS Domain Server	0133
NetWare Naming Service (NNS) Profile	0135
NNS Queue/NW Print Queue	0137
NNS Domain Scheme Descriptor	0138
Intel LANSpool VAP	0141
Aladdin Knowledge	0142
Optical Drives	0143
IrmaLAN Gateway	0152
Named Pipe Server	0154
Intel PICKIT/CAS Talk Server	0168
Unknown (User)	0173
Compaq SNMP Agent	0174
Xtree Server	0180
Xtree	0189
NetWare Access Server	018A
GARP Gateway (Net Research)	01B0
BindView (LAN Support Group)	01B1
Intel LanDesk Manager	01BF
Unknown	01CA
Shiva Netmodem	01CB
LanRover	01CC

Table A-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Castelle FAXPress Server	01D8
Castelle LANPress Print Server	01DA
Unknown	01E4
Legato	01F0
Legato	01F1
SQL Server	0200
NMA Agent (NMS; socket 0x2F90)	0233
LANZ Agent (Socket 0x401F; NetExp)	0237
LANZ Agent (Socket 0x4800)	0238
NMS Hub Management	0239
LANZ Agent (Socket 0x401F)	023A
NetWare SMS (Storage Management System)	023F
NetWare Connect	024E
NMS Console (name-stnMAC+IPX#)	026A
NW4 Time Sync Server (Socket 0x040)	026B
NW4 NDS Server	0278
NetWare for SAA Gateway	0304
Gallacticom BBS	030A
HP LaserJet (Quick Silver)	030C
Attachmate 3270 Gateway	0320
Multi Server Director	0327
Intel NetPort II	0361
ECS Cheyenne ARCserv 5.0 Intel	0375
Cheyenne ARC Serv 5.0 Intel SE	0376
PowerChute Version 3.0 (new)	037E

Table A-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
ViruSafe Notify	037F
HP Bridge	0386
HP Hub	0387
NetWare SAA Gateway	0394
Lotus Notes (OS/2 version)	039B
Central Point Anti Virus NLM	03B7
ARCserve 4.0 (socket 0x 8600)	03C4
Intel LANSpool 3.5	03C7
Lexmark 4033 Print Server	03D5
NetWare SQL/Gupta NLM	03DE
UNIXWare	03E1
UNIXWare	03E4
NetWare File Server Version 4.*x*	0400
NetSprint print server	0414
SiteLock Virus	0429
ARCserve 5.0	044C
Dell SCSI Array (SDA) Monitor	045B
SyBase	0474
SyBase	0475
Novix TCP/IP support NLM	04DC
SiteLock Checks	0520
Certus Anti Virus NLM (master)	0523
SiteLock Checks	0529
Delrina WinFax Pro network	0553
McAfee's NetShield anti-virus	0580

Table A-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
SiteLock	0B29
SiteLock Applications	0C29
SofTrack for NW Version 3.*x*	0C2C
LAI SiteLock	2380
Meeting Maker	238C
SofTrack for NW Version 4.*x*	2C0C
SiteLock Server (Brightworks)	4808
SiteLock User	5555
Tapeware	6312
Rabbit 3270 Gateway	6F00
Intel NetPort (Print Server)	8002
WordPerfect Network Version	8008
Unknown	8069
Unknown	8746
McAfee's NetShield anti-virus	9000
SQL Monitor (IPX)	9604
Unknown	9892
Unknown	C00C
SiteLock Metering VAP/NLM	F11F
SiteLock	F1FF
SQL Server (IPX)	F503

Appendix B
IPX Default Parameter Settings

This appendix lists the default settings for IPX parameters. Use the Configuration Manager to edit any of the default settings listed here.

IPX Global Parameter Defaults

This section describes all parameters shown on the Edit IPX Global Parameters window.

Table B-1. IPX Global Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.15.1.2
Multiple Host Address Enable	Enable	1.3.6.1.4.1.18.3.5.5.15.1.6
Host Number (hex)	If you disable the Multiple Host Address Enable parameter and enter a unique host number, the Configuration Manager assigns this number to all IPX interfaces you configure on the router. If you disable the Multiple Host Address Enable parameter and do not enter a boxwide host ID number for this parameter, the Configuration Manager automatically generates a unique 6-byte host ID number for all IPX interfaces, based on the serial number of the router's backplane.	1.3.6.1.4.1.18.3.5.5.15.1.7
Router Name	None	1.3.6.1.4.1.18.3.5.5.15.1.9
Primary Net Number (hex)	None	1.3.6.1.4.1.18.3.5.5.15.1.5

IPX Advanced Global Parameter Default Values

This section describes all parameters shown on the Edit IPX Advanced Global Parameters window.

Table B-2. IPX Advanced Global Parameter Default Values

Parameter	Default	MIB Object ID
Routing Method	Tick	1.3.6.1.4.1.18.3.5.5.16.1.3
Maximum Path	1 (path)	1.3.6.1.4.1.18.3.5.5.16.1.5
Log Filter	Trace	1.3.6.1.4.1.18.3.5.5.16.1.4
Maximum Path Splits	1 (path)	1.3.6.1.4.1.18.3.5.5.16.1.6
Maximum Hops	1 (hop)	1.3.6.1.4.1.18.3.5.5.16.1.7
Destination Count	1 (destination)	1.3.6.1.4.1.18.3.5.5.16.1.17
Service Count	1 (service)	1.3.6.1.4.1.18.3.5.5.16.1.1
Host Count	1 (host)	1.3.6.1.4.1.18.3.5.5.16.1.21
Aging Frequency	10 (seconds)	1.3.6.1.4.1.18.3.5.5.16.1.23
Aging Pending Frequency	100 (routes and services)	1.3.6.1.4.1.18.3.5.5.16.1.24
Default Route	Disable	1.3.6.1.4.1.18.3.5.5.16.1.25
SAP Via Default Route	Disable	1.3.6.1.4.1.18.3.5.5.16.1.26
Novell Certification Conformance	Enable	1.3.6.1.4.1.18.3.5.5.16.1.15

IPX Interface Parameter Default Values

Any IPX interface you add to a physical circuit inherits a default set of IPX parameter values from the global/slotwide IPX process. You can use the Configuration Manager to access and further modify or customize parameters belonging to a specific interface. This section describes all parameters shown on the IPX Interfaces window.

Table B-3. IPX Interface Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.17.1.2
Name	None	1.3.6.1.4.1.18.3.5.5.17.1.7
Cost	1 (for hop- or tick-based routing)	1.3.6.1.4.1.18.3.5.5.17.1.38

Table B-3. IPX Interface Parameter Default Values *(continued)*

Parameter	Default	MIB Object ID
Host Number	None	1.3.6.1.4.1.18.3.5.5.17.1.25
Configured Encaps	Circuit medium dependent	1.3.6.1.4.1.18.3.5.5.17.1.40
TR End Station	Disable	1.3.6.1.4.1.18.3.5.5.17.1.59
NetBIOS Accept	Disable	1.3.6.1.4.1.18.3.5.5.17.1.60
NetBIOS Deliver	Disable	1.3.6.1.4.1.18.3.5.5.17.1.61
FR Broadcast (hex)	0xFFFFFF	1.3.6.1.4.1.18.3.5.5.17.1.28
FR Multicast (hex)	0xFFFFFF	1.3.6.1.4.1.18.3.5.5.17.1.30
Compress State	Disable	1.3.6.1.4.1.18.3.5.5.17.1.10
Compress Slot	16 (slots)	1.3.6.1.4.1.18.3.5.5.17.1.12
Checksum	Disable	1.3.6.1.4.1.18.3.5.5.17.1.39
SMDS Address (hex)	None	1.3.6.1.4.1.18.3.5.5.17.1.62
IPX Watchdog Spoofing	Disable	1.3.6.1.4.1.18.3.5.5.17.1.64

IPX Change Circuit Parameter Default Values

This section describes how to set all parameters shown on the IPX Change Circuit window. The IPX circuit identifier appears in the window title.

Table B-4. IPX Change Circuit Parameter Default Values

Parameter	Default	MIB Object ID
Configured Network Number	None	1.3.6.1.4.1.18.3.5.5.17.1.22
Configured Encaps	Circuit Medium Dependent	1.3.6.1.4.1.18.3.5.5.17.1.40
Circuit Index	System-assigned	1.3.6.1.4.1.18.3.5.5.17.1.6
IPXWAN	Enable	Not Applicable
Common Network Number	None	1.3.6.1.4.1.18.3.5.5.17.1.24
Negotiated Protocols	Unnumbered RIP	1.3.6.1.4.1.18.3.5.5.17.1.8

IPX RIP Circuit Parameter Default Values

This section describes how to set all parameters shown on the IPX RIP Circuit window. The IPX circuit identifier appears in the window title.

Table B-5. IPX RIP Circuit Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.32.1.2
Mode	Standard	1.3.6.1.4.1.18.3.5.5.32.1.6
Pace	18 (packets/second)	1.3.6.1.4.1.18.3.5.5.32.1.7
Update Interval (sec)	60 (seconds)	1.3.6.1.4.1.18.3.5.5.32.1.8
Age Multiplier	6 (30-second increments, up to a total of 180 seconds)	1.3.6.1.4.1.18.3.5.5.32.1.9
Packet Size	432 (bytes)	1.3.6.1.4.1.18.3.5.5.32.1.10
Use Multicast	Yes	1.3.6.1.4.1.18.3.5.5.32.1.14
Split Horizon	Enable	1.3.6.1.4.1.18.3.5.5.32.1.15
Immediate Update	Enable	1.3.6.1.4.1.18.3.5.5.32.1.17
Default Route Supply	Enable	1.3.6.1.4.1.18.3.5.5.32.1.18
Default Route Listen	Enable	1.3.6.1.4.1.18.3.5.5.32.1.19

IPX SAP Circuit Parameter Default Values

This section describes how to set all parameters shown on the IPX SAP Circuit window. The IPX circuit identifier appears in the window title.

Table B-6. IPX SAP Circuit Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.33.1.2
Mode	Standard	1.3.6.1.4.1.18.3.5.5.33.1.6
Pace	18 (packets/second)	1.3.6.1.4.1.18.3.5.5.33.1.7
Update Interval (sec)	60 (seconds)	1.3.6.1.4.1.18.3.5.5.33.1.8
Age Multiplier	6 (30-second increments, up to a total of 180 seconds)	1.3.6.1.4.1.18.3.5.5.33.1.9
Packet Size	480 (bytes)	1.3.6.1.4.1.18.3.5.5.33.1.10

Table B-6. IPX SAP Circuit Parameter Default Values *(continued)*

Parameter	Default	MIB Object ID
Nearest Server Reply	Yes	1.3.6.1.4.1.18.3.5.5.33.1.11
NSQ Alphabetical	Yes	1.3.6.1.4.1.18.3.5.5.33.1.12
Use Multicast	Yes	1.3.6.1.4.1.18.3.5.5.33.1.16
Split Horizon	Enable	1.3.6.1.4.1.18.3.5.5.33.1.17
Immediate Update	Enable	1.3.6.1.4.1.18.3.5.5.33.1.19

IPX NetBIOS Static Route Configuration Parameter Default Values

This section describes all parameters shown on the IPX NetBIOS Static Route Configuration window.

Table B-7. NetBIOS Static Route Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Server	None	1.3.6.1.4.1.18.3.5.5.27.1.4
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.27.1.5

IPX NetBIOS Static Route Parameter Default Values

This section describes how to set all parameters shown on the IPX NetBIOS Static Routes window.

Table B-8. IPX NetBIOS Static Route Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.27.1.2
Target Server	None	1.3.6.1.4.1.18.3.5.5.27.1.5

Adjacent Host Configuration Parameter Default Values

This section describes all parameters shown on the Adjacent Host Configuration window.

Table B-9. Adjacent Host Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Host Number (hex)	None	1.3.6.1.4.1.18.3.5.5.26.1.5
WAN Address (hex)/ DLCI (decimal)	None	1.3.6.1.4.1.18.3.5.5.26.1.6

IPX Adjacent Hosts Parameter Default Values

This section lists all the parameters shown on the Adjacent Hosts window.

Table B-10. IPX Adjacent Hosts Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.26.1.2
WAN Address (hex)/ DLCI (decimal)	None	1.3.6.1.4.1.18.3.5.5.26.1.6

IPX Static Route Configuration Parameter Default Values

This section describes all parameters shown on the IPX Configuration window.

Table B-11. IPX Static Route Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.19.1.5
Next Hop Host (hex)	None	1.3.6.1.4.1.18.3.5.5.19.1.8

IPX Static Route Parameter Default Values

This section describes how to set all parameters shown on the IPX Static Routes window.

Table B-12. IPX Static Route Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.19.1.2
Hop Count	0	1.3.6.1.4.1.18.3.5.5.19.1.7
Ticks	0	1.3.6.1.4.1.18.3.5.5.19.1.6
Next Hop Host (hex)	None	1.3.6.1.4.1.18.3.5.5.19.1.8

IPX Static Service Configuration Parameter Default Values

This section describes all parameters shown on the IPX Static Services Configuration window.

Table B-13. IPX Static Service Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Service Name	None	1.3.6.1.4.1.18.3.5.5.23.1.5
Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.6
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.7
Host Number (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.8
Socket (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.9

IPX Static Services Parameter Default Values

This section describes how to set all parameters shown on the IPX Static Services window.

Table B-14. IPX Static Services Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.23.1.2
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.7
Host Number (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.8
Socket (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.9
Hop Count	None	1.3.6.1.4.1.18.3.5.5.23.1.10

Route Filter Configuration Parameter Default Values

This section describes all parameters shown on the IPX Route Filter Configuration window.

Table B-15. Route Filter Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.29.1.6
Target Network Mask	None	1.3.6.1.4.1.18.3.5.5.29.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.29.1.13

IPX Route Filter Parameter Default Values

This section describes how to set all the parameters shown on the IPX Route Filters window.

Table B-16. IPX Route Filter Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.29.1.2
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.29.1.6
Target Network Mask	None	1.3.6.1.4.1.18.3.5.5.29.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.29.1.13
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.29.1.8
Protocol	Any	1.3.6.1.4.1.18.3.5.5.29.1.10
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.29.1.9
Cost	None	1.3.6.1.4.1.18.3.5.5.29.1.11

SAP Network Filter Configuration Parameters

This section describes all parameters shown on the IPX Server Network Configuration window.

Table B-17. SAP Network Filter Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.6
Target Network Mask (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.7
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.8
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.30.1.14
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.30.1.9
Protocol	Any	1.3.6.1.4.1.18.3.5.5.30.1.11
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.30.1.10
Cost	None	1.3.6.1.4.1.18.3.5.5.30.1.12

IPX SAP Network-Level Filter Parameter Descriptions

This section describes all parameters shown on the IPX Service Network Filters window.

Table B-18. SAP Network-Level Filter Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.30.1.2
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.6
Target Network Mask (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.7
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.8
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.30.1.14
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.30.1.9
Protocol	Any	1.3.6.1.4.1.18.3.5.5.30.1.11
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.30.1.10
Cost	None	1.3.6.1.4.1.18.3.5.5.30.1.12

IPX Server-Level Filter Configuration Parameter Descriptions

This section describes all parameters shown on the IPX Service Name Filter Configuration window.

Table B-19. IPX Server-Level Filter Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.31.1.2
Target Server	None	1.3.6.1.4.1.18.3.5.5.31.1.6
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.31.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.31.1.13
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.31.1.8
Protocol	Any	1.3.6.1.4.1.18.3.5.5.31.1.10
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.31.1.9
Cost	None	1.3.6.1.4.1.18.3.5.5.31.1.11

IPX SAP Server-Level Parameter Default Values

This section describes how to set all parameters shown on the IPX Server Name Filters window.

Table B-20. IPX SAP Server-Level Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.31.1.2
Target Server	None	1.3.6.1.4.1.18.3.5.5.31.1.6
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.31.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.31.1.13
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.31.1.8
Protocol	Any	1.3.6.1.4.1.18.3.5.5.31.1.10
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.31.1.9
Cost	None	1.3.6.1.4.1.18.3.5.5.31.1.11

Appendix C
Sample IPX Configuration

This appendix provides a sample IPX configuration. Depending on the interface type and service requirements, the network uses different encapsulations. Configurations are provided for Router 1 and Router 2. The network configuration lists Router a and Router b but does not provide configurations for them.

The following assumptions apply:

- The router uses the tick-based RIP method
- The Frame Relay cloud is non-fully meshed and all PVCs are group mode. You have set the management type to default
- You have configured RIP for all interfaces
- You have enabled Multiple Host Addressing under IPX Global
- Default settings are in effect for all timer values

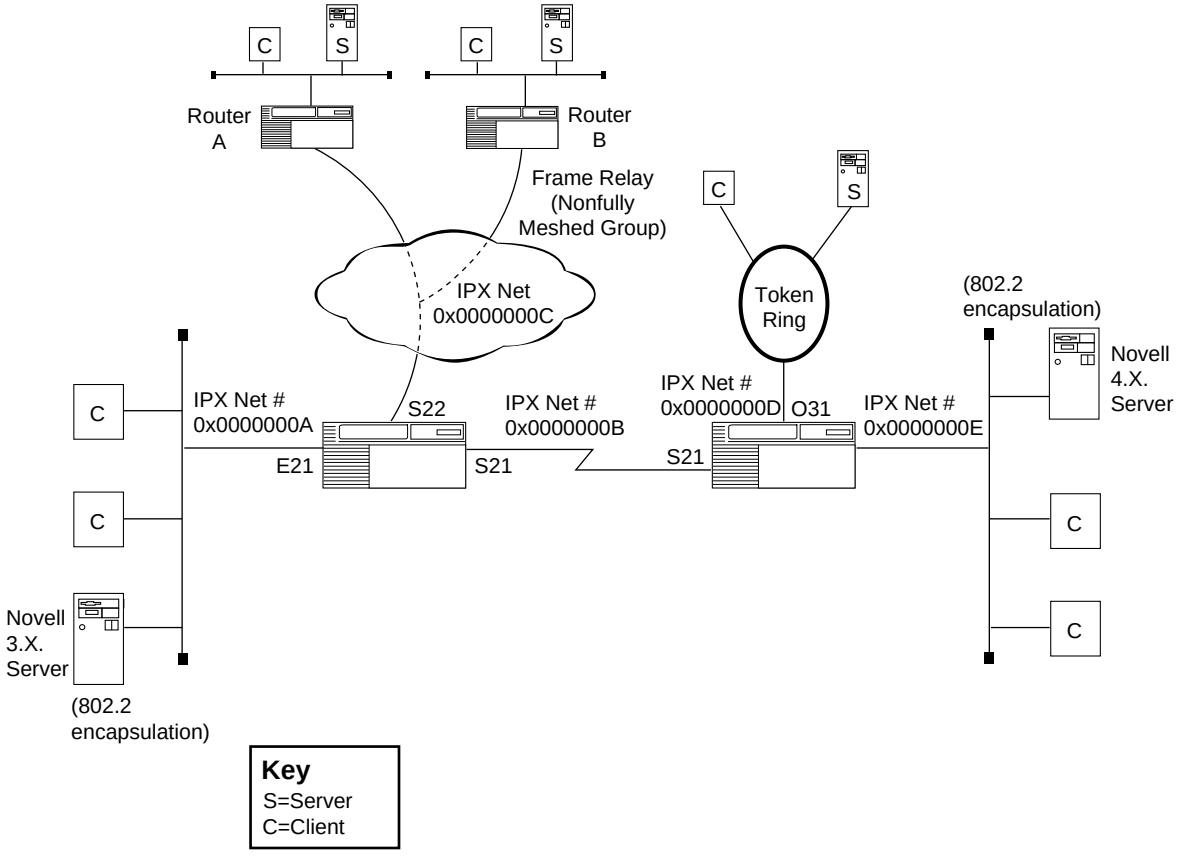

Figure C-1. Sample IPX Configuration

Configuration Particulars

Router 1

Edit the E21 circuit and add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000A and the Configured Encaps parameter to Novell.

Edit the S21 circuit and set the WAN protocol to Standard. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000B.

Edit the S22 circuit and set the WAN protocol to Frame Relay. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000C and click OK. Select **Protocols→IPX→Interfaces**, and highlight the IPX Network parameter, which should be set to 0x0000000C. Click on the RIP button and set the Split Horizon parameter to Disable.

Note: *You should turn off Split Horizon on the Frame Relay hub router if the spoke routers are to learn routes from each other. You should, however, leave Split Horizon enabled on spoke routers.*

Router 2

Edit the E21 circuit and add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000E.

Edit the S21 circuit and set the WAN protocol to Standard. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000B.

Edit the 031 circuit and set the ring speed to 16 MB. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000D and the Configured Encaps parameter to SNAP.

Index

A

accepting
  default configuration parameter values, 3-7

accessing IPX parameters
  using Site Manager, 4-2
  using the Technician Interface, 4-2

Action
  IPX route filter parameter, 4-74
  service name filter parameter, 4-100
  service network filter parameter, 4-90

action
  SAP filters, 1-36

adding
  adjacent hosts, 4-49
  default routes, 4-54
  IPX route filters, 4-69
  NetBIOS static routes, 4-43
  service name filters, 4-93
  service network filter, 4-84
  static routes, 4-54
  static services, 4-59

Adj. Hosts button, 4-48

adjacent host, 1-4, 1-31
  adding, 4-49
  configuration parameter descriptions, 4-50
  deleting, 4-52
  editing, 4-51
  guidelines for configuring, 2-8
  modifying, 4-51
  parameter descriptions, 4-51

adjacent host parameters
  editing, 4-47

advanced global parameters
  descriptions, 4-10
  editing, 4-9

advertisement interval
  RIP, 1-34
  SAP, 1-34

advertisement interval (RIP), 1-20

Age Multiplier
  IPX RIP circuit parameter, 4-34
  IPX SAP circuit parameter, 4-40

aggregation
  route, 1-30

Aging Frequency
  advanced global parameter, 4-15

Aging Pending Frequency
  advanced global parameter, 4-15

ATM
  and adjacent hosts, 1-31
  circuits, 1-16

ATM interface
  configuring IPX on, 2-8

B

bandwidth, 1-17, 1-18, 1-28

Bay Networks
  CompuServe forum, xvi
  customer support, xvi
  Home Page on World Wide Web, xvii
  InfoFACTS service, xvii
  publications, ordering, xix
  Technical Response Center, xviii

bindery
and SAP, 1-33
bridge
source route bridge endstation support, 1-52
Broadcast Address
IPX interfaces parameter, 4-24
broadcast filter
NetBIOS, 1-49
broadcast filtering
NetBIOS, 1-52

C

change circuit parameters
descriptions, 4-27
editing, 4-26
characters in SAP pattern matching filters, 4-78
Circuit Index
IPX change circuit parameter, 4-28
IPX configuration parameter, 3-4
circuit parameters
changing, 4-27
circuits
LAN and WAN, 1-3
client/server connection
example, 1-56
role of Bay Networks router, 1-55
Common Network Number, 1-9
IPX change circuit parameter, 4-29
IPX configuration parameter, 3-5
compatibility with previous versions, 1-1
CompuServe, Bay Networks forum on, xvi
concatenation rules and operators
SAP pattern matching filters, 4-79
configurable RIP timers, 1-20
configurable SAP timers, 1-34
configurable split horizon, 1-26
Configuration Manager window, 4-3
configurations
IPX special, 2-2
IPX standard, 2-1
Configured Encaps
IPX change circuit parameter, 4-28
IPX interface parameter, 4-22
Configured Encaps parameter, 2-4
Configured Network Number
IPX configuration parameter, 3-3
configuring
interface costs, 1-19
RIP and SAP broadcast timers, 1-17
service network filter parameters, 4-81
configuring IPX
on a Token Ring interface, 2-6
on an ATM interface, 2-8
without RIP, 2-8
connection negotiation
IPXCP, 1-11
IPXWAN, 1-12
connectionless datagram protocol, 1-2
Cost
configuring interface costs, 1-19
IPX advanced global parameter, 1-19
IPX interface parameter, 4-20
IPX route filter parameter, 4-75, 4-91, 4-101
tick, 1-15
customer support. *See* getting help

D

data link layer addresses, 2-5
datagram, 1-2
default configuration parameter values
accepting or editing, 3-7
Default Route
advanced global parameter, 4-16
default route, 1-30
adding, 4-54
support, 1-4

Default Route Listen
IPX RIP circuit parameter, 4-36
Default Route Supply
IPX RIP circuit parameter, 4-36
deleting
adjacent host, 4-52
IPX from the router, 4-102
IPX route filters, 4-75
NetBIOS static routes, 4-47
service name filters, 4-101
static routes, 4-58
static services, 4-65
deleting a service network filter, 4-91
Destination Count
advanced global parameter, 4-13
Dial-on-Demand, 1-4, 1-40
with static routing, 1-29, 1-43
with traffic filters, 1-43
dynamic routing, 1-4

E

Edit IPX Advanced Global Parameters window, 4-4, 4-9
Edit IPX Global Parameters window, 4-4
editing
adjacent host parameters, 4-47, 4-51
default configuration parameter values, 3-7
global parameters, 4-3, 4-9
interface parameters, 4-26, B-2
IPX change circuit parameters, 4-26
IPX interface parameters, 4-17
IPX parameters, 4-1
IPX RIP circuit parameters, 4-30
IPX route filter parameters, 4-71
IPX SAP circuit parameters, 4-37
NetBIOS static routes, 4-46
route filter configuration parameters, 4-69
service name filter parameters, 4-92
service name filters, 4-96
service network filters, 4-86
static route parameters, 4-52, 4-56
static routes, 4-52
static service parameters, 4-58, 4-63
editing IPX advanced global parameters, 4-9
editing IPX global parameters, 4-3
Enable
adjacent host parameter, 4-51
IPX global parameter, 4-5
IPX interface parameter, 4-19
IPX NetBIOS static route parameter, 4-46
IPX RIP circuit parameter, 4-32
IPX route filter parameter, 4-72
IPX SAP circuit parameter, 4-38
IPX static route parameter, 4-56
IPX static service parameter, 4-64
service name filter parameter, 4-97
service network filter parameter, 4-87
enabling
IPX and IPXWAN, 3-1
encapsulation method, 1-5
encapsulation types. *See* frame encapsulation types
endstation support, 1-15, 1-52

F

filter
adding service network filters, 4-84
deleting service name filters, 4-101
editing service name filters, 4-92, 4-96
editing service network filters, 4-86
NetBIOS broadcast, 1-49
route, 1-17
route filters, 4-66
SAP, 1-36
SAP filter concatenation rules and operators, 4-79
SAP filter pattern matching, 1-36
SAP filtering example, 4-81
SAP filters prohibiting SAP broadcasts, 1-40
SAP filters with pattern matching, 4-77
SAP pattern matching characters, 4-78

service name filter configuration parameters, 4-94
service network filter parameters, 4-81, 4-87
traffic filters with dial-on-demand, 1-43
Filter Priority
IPX route filter configuration parameter, 4-71
IPX route filter parameter, 4-73
service name filter configuration parameter, 4-96
service name filter parameter, 4-98
service network configuration parameter, 4-86, 4-88
filters
SAP filters with wildcards, 4-76
frame encapsulation types, 2-4
frame formats, 1-3
Frame Relay, 1-7, 1-8
and adjacent hosts, 1-31
circuits, 1-16
fully meshed network, 1-27
split horizon enabled, 1-27

G

getting help
from a Bay Networks Technical Response Center, xviii
through CompuServe, xvi
through InfoFACTS service, xvii
through World Wide Web, xvii
global parameters
advanced, descriptions, 4-10
advanced, editing, 4-9
descriptions, 4-5
editing, 4-3, 4-9

H

HDLC encapsulation, 1-19
hop
as basis for routing decision, 1-14
definition, 4-11
RIP maximum, 1-19
Hop Count
IPX static route parameter, 4-57
IPX static service parameter, 4-65
hop count, 4-11
host
adjacent, 1-31, 4-49
next hop host, 4-55, 4-57
Router Host Number parameter, 4-7
Host Count
advanced global parameter, 4-14
host ID numbers
on a Token Ring circuit, 2-6
Host Number
adjacent host parameter, 4-50
IPX interface parameter, 4-21
IPX static service parameter, 4-62, 4-64
host numbers, 2-3

I

Immediate Update
IPX RIP circuit parameter, 4-36
IPX SAP circuit parameter, 4-42
InfoFACTS service, xvii
information broadcast
RIP, 1-16
interface costs
configuring, 1-19
interface number. *See* circuit index.
interface parameters
descriptions, 4-19
editing, 4-17, 4-26, B-2
Internet Data Packet (IDP) format, 1-2
Internet Packet Exchange. *See* IPX
internetwork addressing, 1-2
intranode addressing, 1-2
IPX
background information, 1-58
configuring without RIP, 2-8

deleting IPX from the router, 4-102
enabling, 3-1
parameters
Cfg Encaps, 3-4
Configure RIP, 3-4
Network Address (hex), 3-3
IPX Adjacent Host Configuration window, 4-49
IPX Adjacent Hosts window, 4-48
IPX advanced global parameters
descriptions, 4-10
editing, 4-9
IPX change circuit parameters, 4-26
descriptions, 4-27
IPX Change Circuit window for IPXWAN, 4-26
IPX Configuration window, 3-2
IPX configurations
multiple interfaces per circuit, 2-2
special, 2-2
standard, 2-1
IPX global parameters
descriptions, 4-5
editing, 4-3
IPX interface parameters
descriptions, 4-19
editing, 4-17
IPX Interfaces window, 4-18
IPX NetBIOS Static Route Configuration window, 4-44
IPX NetBIOS Static Routes window, 4-43
IPX NetBIOS static routing, 1-44
IPX network
sample (figure), 1-57
IPX over WAN media, 1-4, 1-6
link configurations, 1-12
IPX overview, 1-2
IPX parameters
accessing via Site Manager, 4-2
accessing via Technician Interface, 4-2
editing, 4-1
IPX ping, 1-15
IPX ping support, 1-54
IPX RIP circuit parameters
descriptions, 4-32
editing, 4-30
IPX RIP Circuit window, 4-31
IPX Route Filter Configuration window, 4-69
IPX route filter parameters
descriptions, 4-71
editing, 4-71
IPX route filters, 1-17
IPX Route Filters window, 4-67
IPX SAP circuit parameters
descriptions, 4-38
editing, 4-37
IPX SAP Circuit window, 4-37
IPX Server Network Filter Configuration window, 4-84
IPX service name filter
configuration parameter descriptions, 4-94
parameter descriptions, 4-97
IPX Service Name Filter Configuration window, 4-94
IPX Service Name Filters window, 4-92
IPX service network filter parameters
descriptions, 4-87
IPX Service Network Filters window, 4-82
IPX Static Route Configuration window, 4-54
IPX static service
configuration parameter descriptions, 4-60
parameter descriptions, 4-63
IPX Static Services window, 4-59
IPX watchdog acknowledgment, 1-43
IPX Watchdog Spoofing
IPX interface parameter, 4-25

IPXCP, 1-4, 1-7
  link configurations, 1-12
  link negotiation, 1-11
  sample configuration, 1-10
  using, 1-7
IPXWAN, 1-4, 1-7
  configuring without RIP, 2-8
  enabling, 3-1
  IPX change circuit parameter, 4-29
  IPX configuration parameter, 3-5
  link configurations, 1-12
  link negotiation, 1-12
  sample configuration, 1-10
  using, 1-7
IPXWAN connection
  negotiating, 1-8

L

LAN
  circuits, 1-3
  logical, 1-5
  physical, 1-5
link delay
  WAN link, 1-8
link negotiation, 1-7
  IPXCP, 1-11
  IPXWAN, 1-12
load redistribution and rerouting, 1-24
load sharing, 1-15, 1-22, 1-24
Local IPX watchdog acknowledgment, 1-43
Log Filter
  advanced global parameter, 4-12
logical LAN, 1-5
logical network address, 1-5

M

MAC Address Override parameter, 2-2, 2-3, 2-7
MAC Address Select parameter, 2-2, 2-3, 2-7
MAC addresses, 2-3
Maximum Hops
  advanced global parameter, 4-13
Maximum Path
  advanced global parameter, 4-12
  IPX advanced global parameter, 1-23
Maximum Path Splits
  advanced global parameter, 4-12
Mode
  IPX RIP circuit parameter, 4-33
  IPX SAP circuit parameter, 4-39
  service name filter parameter, 4-99
  service network filter parameter, 4-89
modifying
  adjacent host, 4-51
  NetBIOS static routes, 4-46
  service name filters, 4-96
  service network filters, 4-86
  static routes, 4-56
  static services, 4-63
Multicast Address
  IPX interface parameter, 4-24
multiline, 2-1
multiline circuits, 1-25
  differences from multipath, 1-26
multipath configurations, 1-25
multipath routing, 1-15, 1-22, 4-12
  precedence/priority, 1-25
multiple circuits per segment, 2-1
Multiple Host Address Enable
  IPX global parameter, 4-6
Multiple Host Address Enable parameter, 2-1, 2-3
multiple interfaces per circuit, 1-5, 2-1, 2-2
multiple IPX interfaces per circuit, 1-4
Multiple-Host addressing, 2-3
multiple-host router, 2-1

N

Name
  IPX interface parameter, 4-19
NCP
  Network Control Protocol, 1-7
NDS (NetWare Directory Services, 1-33
Nearest Server Reply
  IPX SAP circuit parameter, 4-41
Negotiated Protocol(s)
  IPX change circuit parameter, 4-30
  IPX configuration parameter, 3-6
negotiation
  IPXCP link, 1-11
  IPXWAN connection, 1-8
  IPXWAN link, 1-12
NetBIOS
  broadcast packet (Type 20), 1-45
  Type 20 broadcast packets, 1-15
NetBIOS Accept, 1-47, 1-49
  IPX interface parameter, 4-23
NetBIOS broadcast filtering, 1-49, 1-52
NetBIOS Deliver, 1-47, 1-49
  IPX interface parameter, 4-23
NetBIOS packet
  filtering, 1-50
  use with nonstandard static routing, 1-46
  use with standard static routing, 1-48
NetBIOS packet flow, 1-51
NetBIOS static routes, 1-44, 1-46
  adding, 4-43
  configuration parameter descriptions, 4-44
  deleting, 4-47
  editing, 4-46
  modifying, 4-46
  parameter descriptions, 4-46
NetWare
  bindery, 1-33
  Directory Services (NDS), 1-33
  Novell, 1-6
Network
  IPX static service parameter, 4-62
network
  fully meshed, 1-27
  nonfully meshed, 1-27
network address
  logical, 1-5
Network Control Protocol (NCP), 1-7
network number, 1-8
  primary, 1-9
network number field
  IPX RIP packet, 1-17
network numbers
  common, 2-4
  primary, 2-4
  setting for IPXCP, 2-4
  setting for IPXWAN, 2-4
network-level services, 1-4
Next Hop Host
  IPX static route configuration parameter, 4-55
  IPX static route parameter, 4-57
nonfully meshed network, 1-27
  split horizon disabled, 1-28
Novell
  NetWare, 1-6
  standards, 1-18
Novell Certification Conformance
  advanced global parameter, 4-17
Novell, Inc., 1-2
number of IPX interfaces per circuit, 2-4

O

OSI model, 1-1

P

Pace
  IPX RIP circuit parameter, 4-33
  IPX SAP circuit parameter, 4-39

Packet Size
IPX RIP circuit parameter, 4-34
IPX SAP circuit parameter, 4-40
parameters
editing IPX parameters, 4-1
IPX
Cfg Encaps, 3-4
Configure RIP, 3-4
pattern matching
concatenation rules and operators, 4-79
SAP filters, 1-36, 4-77
periodic RIP advertisement interval, 1-20
periodic SAP advertisement interval, 1-34
Permanent Virtual Circuit (PVC), 1-8
physical LAN, 1-5
ping, 1-54
ping capability, 1-15
PNN (primary network number), 1-9
PPP (point-to-point protocol), 1-7
precedence/priority
multipath routing, 1-25
primary link, 1-8
IPXWAN link negotiation, 1-12
Primary Net Number
IPX global parameter, 4-8
primary network number (PNN), 1-9
primary router, 1-8
Protocol
IPX route filter parameter, 4-74
service name filter parameter, 4-99
service network filter parameter, 4-89
protocol type. *See* negotiated protocols
purging
RIP entries, 1-21
SAP entries, 1-34
PVC (Permanent Virtual Circuit), 1-8

R

regular expression (RE), 4-77
request packet (RIP), 1-15
response packet (RIP), 1-15
RFC
IPX source documents, 1-58
RFC 1552, 1-7, 1-58
RFC 1634, 1-7, 1-58
RIF (Routing Information Field), 1-53
RIP, 1-14, 1-15
RIP (Routing Information Protocol), 1-4
listen and supply functions, 1-16
maximum timer ticks, 1-19
update packet transmissions frequency, 1-17
RIP broadcast timers
configuring, 1-17
RIP circuit parameters
descriptions, 4-32
editing, 4-30
RIP information broadcast, 1-16
RIP interface parameters. *See* RIP circuit parameters, editing
RIP request packet, 1-15
RIP response packet, 1-15
RIP timers
configurable, 1-20
RIP WAN, 3-6
route aggregation, 1-30
Route Filter button, 4-67
route filter configuration parameters
editing, 4-69
route filters, 1-17
adding, 4-69
deleting, 4-75
dropping all routes, 4-68
parameter descriptions, 4-71
parameter editing, 4-71
using, 4-66

router
deleting IPX from the router, 4-102
multiple-host, 2-1
primary, 1-8
secondary, 1-8
single-host, 2-1, 2-2
Router Host Number
IPX global parameter, 4-7
Router Host Number parameter, 2-2
router information broadcast, 1-16
Router Name
IPX global parameter, 4-8
router name
valid characters in, 1-10
routes
dropping all, 4-68
Routing Information Field (RIF), 1-53
Routing Information Protocol (RIP), 1-4, 1-14, 1-15
Routing Method
advanced global parameter, 4-11
IPX advanced global parameter, 1-19
routing methods, 1-19
routing table, 1-15, 1-16
running IPX over Frame Relay, 1-8
running IPX over PPP and Frame Relay, 1-7

S

SAP, 1-14, 1-32
and NDS, 1-33
and the NetWare bindery, 1-33
timeout, 1-34
SAP (Service Advertising Protocol), 1-4
SAP advertisement interval, 1-34
SAP broadcast timers
configuring, 1-17
SAP filters, 4-79
editing service network filters, 4-86
example, 4-81
pattern matching, 1-36, 4-77
pattern matching characters, 4-78
prohibiting SAP broadcasts, 1-40
service network configuration parameters, 4-84
setting up, 4-76
wildcards and pattern matching, 4-76
SAP service
adding, 4-59
configuration parameters, 4-60
deleting, 4-65
SAP timer
configurable, 1-34
SAP update packet transmissions frequency, 1-17
SAP Via Default Route
advanced global parameter, 4-16
secondary router, 1-8
Service Advertising Protocol (SAP), 1-4, 1-14, 1-32
Service Count
advanced global parameter, 4-14
Service Name
IPX static service parameter, 4-61
service name filter parameters
editing, 4-92
service name filters
adding, 4-93
configuration parameter descriptions, 4-94
deleting, 4-101
editing, 4-96
modifying, 4-96
parameter descriptions, 4-97
service network filter
adding, 4-84
configuration parameter descriptions, 4-84
editing, 4-86
modifying, 4-86
service network filter parameters
configuring, 4-81
descriptions, 4-87
editing, 4-81

service network filters
dropping all services, 4-83
Service Type
IPX static service parameter, 4-61
service types, A-1
services
dropping all, 4-83
Single Route Explorer (SRE) frame, 1-53
single-host router, 2-1, 2-2
Site Manager, 1-1
accessing IPX parameters, 4-2
slave router. *See* secondary router.
SMDS
and adjacent hosts, 1-31
circuits, 1-16
Socket
IPX static service parameter, 4-62, 4-65
numbers, 1-2
source route bridge endstation support, 1-52
source routing, 1-15
special IPX configurations
multiple circuits per segment, 2-5
multiple interfaces per circuit, 2-2
Split Horizon
IPX RIP circuit parameter, 4-35
IPX SAP circuit parameter, 4-41
split horizon, 1-15
configuring, 1-26
disabled in a nonfully meshed network, 1-28
enabled in a fully meshed network, 1-27
SRE frame, 1-53
standard IPX configurations
multiple-host router, 2-1
single-host router, 2-2
static routes, 1-28
adding, 4-54
adding a NetBIOS static route, 4-43
configuration parameter descriptions, 4-55
deleting, 4-58
deleting NetBIOS static routes, 4-47
editing NetBIOS static routes, 4-46
guidelines for configuring, 2-8
modifying, 4-56
NetBIOS, 1-44, 1-46
NetBIOS configuration parameters, 4-44
nonstandard NetBIOS use, 1-46
parameter descriptions, 4-56
parameter editing, 4-56
support, 1-4
using, 4-52
with Dial-on-Demand, 1-43
with standard NetBIOS routing, 1-48
static service configuration parameters
descriptions, 4-60
static service parameters
editing, 4-58, 4-63
static services, 1-37
adding, 4-59
deleting, 4-65
modifying, 4-63
parameter descriptions, 4-63
SAP service network configuration, 1-39

T

Target Network
IPX NetBIOS static route parameter, 4-45, 4-47
IPX route filter configuration parameter, 4-70
IPX route filter parameter, 4-72
IPX static route configuration parameter, 4-55
IPX static service parameter, 4-64
SAP network-level filter parameter, 4-87
service network configuration parameter, 4-85
Target Network Mask
IPX route filter configuration parameter, 4-70
IPX route filter parameter, 4-73
service network configuration parameter, 4-85, 4-88
Target Server
IPX NetBIOS static route parameter, 4-45

Target Service Name
service name filter configuration parameter, 4-95
service name filter parameter, 4-97
Target Service Type
service name filter configuration parameter, 4-95
service name filter parameter, 4-98
service network configuration parameter, 4-85, 4-88
Technician Interface
accessing IPX parameters, 4-2
tick
as basis for routing decision, 1-14
cost, 1-15
definition, 1-15, 4-11
RIP timer maximum, 1-19
tick-based routing, 1-8
Ticks
IPX static route parameter, 4-57
timeout
RIP entries, 1-21
SAP entries, 1-34
timer
configurable SAP timers, 1-34
RIP (configurable), 1-20
RIP and SAP broadcast, 1-17
Token Ring
configuring host ID numbers, 2-6
Token Ring interface
configuring IPX on, 2-6
Token Ring line detail parameters
MAC Address Override, 2-2, 2-3, 2-7
MAC Address Select, 2-2, 2-3, 2-7
Token-Ring
endstation support, 1-52
TR End Station
IPX interface parameter, 4-22
traffic filters
with Dial-on-Demand, 1-43
Type 20 broadcast packet
NetBIOS, 1-15, 1-45

U

Unnumbered RIP, 1-4, 3-6
Update Interval
IPX RIP circuit parameter, 1-18, 4-34
IPX SAP circuit parameter, 1-18, 4-40
upper-layer protocol
handling packets associated with, 1-14
Use Multicast
IPX RIP circuit parameter, 4-35
IPX SAP circuit parameter, 4-41

W

WAN
circuits, 1-3
link delay, 1-8
media, 1-7
SAP announcements, eliminating, 4-58
WAN Address (hex)/DLCI (decimal)
adjacent host parameter, 4-50, 4-52
WAN NLSP, 3-6
watchdog acknowledgment, 1-43
watchdog spoofing parameter, 4-25
wildcards
with SAP filters, 4-76
World Wide Web, Bay Networks Home Page on, xvii

X

Xerox Network System (XNS), 1-2